TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Helen Ojamaa-Muru

PÕHIÕIGUSTE JA -VABADUSTE KAITSE RIIGI INFOSÜSTEEMI AMETI JÄRELEVALVE VOLITUSTE LAIENDAMISEL

Magistritöö

Juhendaja
Dr.iur Eneken Tikk

Tallinn
2018

SISUKORD

SISSEJUHATUS

Tehnoloogia, sealhulgas infotehnoloogia, areng on füüsilise ruumi kõrvale loonud küberruumi. See on inimkonnale pakkunud järjest uusi võimalusi. Eesliide küber- viitab omavahel ühenduses olevatele infotöötlusvahenditele ja -süsteemidele. Küberruumi omakorda saab käsitada kui tehnoloogia abil loodavat ja tunnetatavat reaalsust ja küberruumis turvalist olekut ehk küberturvalisust seisundina, mille puhul infotöötlusvahendeid mõjutavad riskid ei realiseeru.[1] Uued võimalused toovad aga kaasa uut laadi probleeme. Küberturvalisuse teema tõusis teravalt päevakorda 2007. aastal Eesti ja 2008. aastal Gruusia vastu suunatud küberrünnakute tõttu. Rünnakud tõestasid, et isegi kui agressiivne tegevus toimub küberruumis, võivad tagajärjed olla väga tõsised, ulatudes reaalsesse maailma ja ohustades ühiskonna tavapärast toimimist. Sellised rünnakud võivad kujutada ohtu riigi julgeolekule. Küberrünnakute kõrval on levinud erinevad pahatahtliku kübertegevuse vormid, mis küll ei kujuta otsest ohtu elule ja tervisele, kuid millega võivad ohvrile kaasneda märkimisväärsed ebameeldivused, materiaalne või moraalne kahju jm soovimatud tagajärjed, näiteks lunaraha nõudmine. Kahtlemata on turvaline küberruum ka ühiskonna huvides. Kuivõrd see ei vasta tavaarusaamale avalikust ruumist, siis vajab arutelu, milliste meetmetega on küberruumis turvalisuse tagamine legitiimne ning millistest õigustest ja hüvedest ollakse teatud ulatuses valmis turvalisuse nimel loobuma.

Ka inimõiguste kaitse on üle maailma suurima tähelepanu all kui kunagi varem. Inimõiguste hulka kuuluvad põhiõigused ja -vabadused on kujunenud arvukaiks ning nende olulisus ja rahvusvaheline tunnustatus on olulisel määral muutunud. Levinud on arvamus, et ka ligipääs internetile on kujunenud inimõiguseks. Erinevad infotehnoloogilised lahendused on avanud uued võimalused näiteks riigivalitsemises ja sõnavabaduse teostamises. Kaasaegses demokraatlikus ühiskonnas peetakse inimõiguste tagamist riigi toimimise üheks alustalaks. Põhiõigused ja -vabadused omandatakse sünniga ning on igal inimesel võõrandamatud, kuigi teatud tingimustel – ka turvalisuse tagamiseks – on võimalik ja vajalik neid piirata. Kahe nimetatud teemavaldkonna koosmõjus tõusetuvad aktuaalsed küsimused: kas üksikisiku põhiõiguste ja -vabaduste piiramine küberturvalisuse tagamisel on õigustatud ning millistel tingimustel ja ulatuses on see legitiimne, kui kaalul on riigi või rahvusvahelise kogukonna huvid.

[1] Eesti Vabariigi Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014–2017 lisa 2, lk 4, 6. – https://www.mkm.ee/sites/default/files/lisa_2_valdkondlik_metoodika.doc (21.04.2018).

Küberturvalisus on globaalset olemust arvestades olnud peamiselt rahvusvahelise õiguse valdkonda kuuluv, puudutades selle erinevaid harusid, näiteks riigivastutusõigust, relvastatud jõu kasutamise õigust jm. Inimõigusi kaitstakse rahvusvahelise õigusega, aga ka riigisisese õigusega. Eesti õiguskorras sisalduvad vastavad alused Eesti Vabariigi põhiseaduses[2] (edaspidi ka põhiseadus või PS). Kuigi mõlemad valdkonnad on riikide ülese iseloomuga, on rakenduspraktikas suur roll riigisisesel õigusel. Lisaks tuleb arvestada, et tehnoloogia areng on kiire, mis esitab küberruumi õiguslikule reguleerimisele suure väljakutse. Järjest võetakse kasutusele uusi tehnoloogilisi lahendusi, kuid olemasolev õiguslik raamistik ei pruugi tehnoloogia arengu kiirusega kaasas käia.[3]

Käesolevas töös analüüsib autor küberruumis turvalisuse ja julgeoleku tagamisega kaasnevat riivet seoses põhiõiguste ja -vabaduste kaitse kohustusega. Magistritöö keskne probleem on selgitada välja, kas ja millises ulatuses on Riigi Infosüsteemi Ameti (edaspidi RIA) riikliku järelevalve volituste laiendamisel arvestatud põhiõiguste ja -vabaduste kaitsega. Autor püstitab eesmärgi selgitada välja, millised suundumused ohustavad Eestit küberruumis ja hinnata riikliku järelevalve raames rakendatavate meetmetega kaasnevat mõju. Hüpoteesi kohaselt on Eestis küberruumis turvalisuse tagamiseks planeeritud ulatuslikud riikliku järelevalve meetmed, kuid kaasnev põhiõiguste ja -vabaduste riive pole kõigi meetmete puhul eesmärgi suhtes proportsionaalne.

Põhiõiguste ja -vabaduste kaitse olulisus ning käesoleva töö aktuaalsus on seotud muuhulgas ka analüüsi fookuses oleva küberturvalisuse seaduse eelnõuga[4] (edaspidi ka KüTS eelnõu), kus on kaitse vajadus otsesõnu välja toodud (KüTS eelnõu § 6 punkt 5). Siiski ilmneb, et küberturvalisuse seaduse eelnõu ettevalmistamise käigus pole riikliku järelevalve meetmete planeerimisel nendega kaasnevat riivet põhjalikult analüüsitud.[5] Demokraatlikus riigis peavad avaliku võimu rakendatavad piirangud olema legitiimsed ja nendega kaasnev riive põhjendatud. Eesti õiguses on riiklik järelevalve keskselt reguleeritud korrakaitseseaduses, moodustades koos valdkondlikes seadustes sisalduvate erinormidega korrakaitseõiguse terviku. Küberturvalisuse valdkonnas on riikliku järelevalve erimeetmed sätestatud peamiselt küberturvalisuse seaduse eelnõus. Korrakaitseõiguse põhine riikliku järelevalve toimimine ei

[2] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
[3] E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura, 2007, lk 25.
[4] Küberturvalisuse seaduse eelnõu (kuupäevaga 03.10.2017 ametlikule kooskõlastamisele esitatud versioon). – https://eelnoud.valitsus.ee/main/mount/docList/e7ff643b-8b72-4a70-8f3e-dab03f9ca79f (21.04.2018).
[5] Vt küberturvalisuse seaduse eelnõu seletuskiri (viide 88). Eelnõu seletuskiri avab riikliku järelevalve meetmetega seotud riive küsimusi vaid mõnel leheküljel (seletuskirja lk 23–26) ega viita põhjalikumale analüüsile. Sealjuures on veidi pikemalt selgitatud vaid eelnõu §-s 17 reguleeritud küberintsidendi tõkestamist. Sama probleem tuuakse välja ka eelnõu ametlikul kooskõlastamisel (vt näiteks eelnõu seletuskirja lisa 3, lk 30, kättesaadav eelnõude infosüsteemis).

pruugi aga olla valdkondade eripärade tõttu igal elualal ühtviisi sobiv. Seetõttu on vaja välja selgitada, kas valitud reguleerimise loogika võimaldab piisavalt ulatuslikult küberruumi turvalisust ohustavaid sündmusi ära hoida või nende mõjusid piirata.

Hüpoteesi kontrollimiseks on püstitatud kolm uurimisküsimust. Esiteks, millised suundumused mõjutavad küberruumi turvalisust ja millist õigust saab turvalisust ohustavate sündmuste korral kohaldada. Sealjuures on tõstatatud ka küsimus korrakaitseõiguse piiridest. Eesti õiguses annavad korrakaitseseadus[6] (edaspidi ka KorS), hädaolukorra seadus[7] (edaspidi ka HOS), erakorralise seisukorra seadus[8] ning riigikaitseseadus[9] võimalused kehtestada põhiõigusi ja -vabadusi piiravad meetmed riigis julgeoleku ja avaliku korra tagamiseks. Nimetatud seadused ei näe aga selgesõnaliselt ette meetmeid küberruumis kohaldamiseks. Elektroonilise side seadusega[10] (edaspidi ka ESS) on sideettevõtjale sätestatud kohustus sidevõrkude ja -teenuste turvalisuse ning terviklikkuse tagamiseks. Siiski sisaldab see piiratud võimalusi meetmete rakendamiseks küberruumis. Teiseks, kuivõrd on küberturvalisuse valdkonnas rakendatavad riikliku järelevalve meetmed kooskõlas põhiseadusega. Sellega seoses analüüsitakse küberturvalisuse seaduse eelnõus reguleeritud riikliku järelevalve meetmeid põhiõiguste ja -vabaduste kaitse tagamise seisukohast. Autor uurib, kui kaugele lubab põhiseadus piirangutega minna, et tagada küberruumis julgeolek ja avalik kord. Viimase uurimisküsimuse raames uuritakse, kas ja milliseid riikliku järelevalve meetmeid tuleks muuta või täiendavalt kehtestada, et küberruumis turvalisuse tagamise eesmärk oleks tasakaalus põhiõiguste ja -vabaduste kaitsega. Autor kasutab magistritöös kvalitatiivset analüüsimetoodikat.

Õiguskirjanduses on küberturvalisuse valdkonda Eesti riigisisese õiguse seisukohast vähe käsitletud ning sarnasel teemal ei ole akadeemilisi töid autorile teadaolevalt kirjutatud. Küberturvalisuse teemat on avatud peamiselt rahvusvahelise õiguse kontekstis. Suure panuse õiguslikku analüüsi on andnud NATO küberkaitsekoostöö keskuse analüüsid ja raportid. 2017. aastal ilmus keskuse eestvedamisel põhjalik küberruumis kohalduva rahvusvahelise õiguse käsiraamat *Tallinn Manual 2.0*[11], mis on järg 2013. aastal ilmunud käsitlusele. Käsiraamat leidis kasutust ka käesolevas analüüsis, kuid vähesel määral, arvestades analüüsitavate küsimuste riigisisest fookust. Eesti korrakaitseõiguse ülesehitust on varem analüüsitud kahe doktoritöö

[6] Korrakaitseseadus. – RT I, 02.12.2016, 6.
[7] Hädaolukorra seadus. – RT I, 03.03.2017, 1.
[8] Erakorralise seisukorra seadus. – RT I, 12.03.2015, 12.
[9] Riigikaitseseadus. – RT I, 27.06.2017, 6.
[10] Elektroonilise side seadus. – RT I, 01.07.2017, 2.
[11] M. N. Schmitt (gen.ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : prepared by the International Groups of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press 2017.

raames: M. Laaring[12] ohuennetusõiguse ja J. Jäätma[13] ohutõrjeõiguse aspektist. Mõlemad väitekirjad annavad korrakaitseõiguse vastavast aspektist põhjaliku ülevaate, mistõttu toob autor käesolevas töös nendest välja teema avamise seisukohast põhilise ega käsitle mahupiirangu tõttu korrakaitseõiguse teooriat detailselt. Põhiseadusega tagatud põhiõiguste ja -vabaduste sisu tõlgendamisel kasutab autor põhiseaduse kommenteeritud väljaande 2017. aastal ilmunud versiooni. Samuti leiavad töös kasutust asjakohased Riigikohtu lahendid ning meetmeid analüüsitakse Riigikohtu tunnustatud proportsionaalsuse testi meetodil. Küberruumis avalduvatest suundumustest ülevaate andmiseks kasutatakse rahvusvaheliste organisatsioonide ja Eesti ametkondade küberturvalisuse raporteid. Viimased on kõrge üldistusastmega avalikud dokumendid, mida autor kasutab õiguslike küsimuste avamiseks olulise taustinformatsiooni andmiseks.

Magistritöö koosneb kolmest peatükist. Esimeses peatükis antakse ülevaade Eesti korrakaitseõiguse ning põhiõiguste ja -vabaduste kaitse teoreetilistest alustest, mis moodustab raamistiku edasisele analüüsile. Teemasid avades selgitatakse nende kohati konkureerivat olemust. Põhiseadus on ette näinud põhiõiguste ja -vabaduste kaitse kohustuse aga ka vastava riive võimalikkuse muuhulgas avaliku korra ja julgeoleku tagamiseks. Siiski peab riivel olema seaduslik alus ja riivavat meedet kohaldava korrakaitseorgani tegevus peab igal üksikjuhtumil olema põhjendatud ning proportsionaalne eesmärgi suhtes. Teises peatükis käsitletakse küberruumi turvalisust mõjutavaid suundumusi. Probleemide kaardistuse põhjal analüüsitakse nendega toimetulekuks asjakohast õigusraamistikku. Eesmärk on selgitada välja, millist laadi ja millises ulatuses on küberturvalisusega seotud probleeme võimalik riikliku järelevalvega lahendada. See avab tausta, miks on vaja piiravaid meetmeid rakendada ning põhiõigusi ja -vabadusi riivata. Autor peab vajalikuks avada pikemalt korrakaitseseaduse mõisteid ja nende seoseid küberturvalisuse valdkonnaga. Korrakaitseseaduses defineeritud mõisted oht, avalik kord, korrarikkumine jt on korrakaitseõiguse kesksed, mistõttu ka küberturvalisuse valdkonnas kasutatavad mõisted peavad olema korrakaitseseaduses kasutatavaga vastavuses, et seosed riikliku järelevalve korraldusega oleksid selged. Viimases, kolmandas peatükis analüüsitakse küberturvalisuse valdkonnas rakendatavaid riikliku järelevalve meetmeid põhiseadusega tagatud põhiõiguste ja -vabaduste kaitse seisukohast. Proportsionaalsuse testi läbiviimisega hinnatakse iga meetme sobivust, vajalikkust ja mõõdukust ning tehakse vajadusel ettepanekud nende täiendamiseks. Analüüsi koondtulemusena annab autor hinnangu, kuivõrd RIA

[12] M. Laaring. Eesti korrakaitseõigus ohuennetusõigusena. Tartu: Tartu Ülikooli Kirjastus 2015.
[13] J. Jäätma. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu: Tartu Ülikooli Kirjastus 2015.

järelevalvepädevuse laiendamisega küberturvalisuse valdkonnas on tagatud põhiõiguste ja -vabaduste kaitse. Magistritööga soovib autor küberturvalisuse seaduse eelnõus sätestatud riikliku järelevalve meetmeid analüüsides anda oma panuse, et aidata kaasa küberturvalisuse valdkonna tasakaalustatud reguleerimisele.

Märksõnad: küberturve, avalik kord, põhiõigused.

1. PÕHIÕIGUSTE JA -VABADUSTE KAITSE NING AVALIKU KORRA TAGAMINE

1.1. Põhiõigused ja -vabadused Eesti Vabariigi põhiseaduses

R. Alexy märgib põhiseaduse analüüsis, et põhiõigused on samaaegselt nii riikliku õiguskorra osa kui ka põhimõtted, mida tunnustatakse laiemalt kui riigi tasand, sealhulgas olles nii rahvusvahelise õiguse kui ka Euroopa Liidu õiguse reguleerimisobjektiks. Õiguste kandja põhjal saab eristada igaühele kuuluvaid inimõiguseid, konkreetse riigi kodanikele kuuluvaid kodanikuõiguseid ja rahvuse alusel isikule kuuluvaid rahvusõiguseid. Põhiõigused sisaldavad inimõiguseid, mis on oma olemuselt universaalsed ja peaksid kehtima kõikjal, olenemata konkreetsest õiguskorrast.[14] Inimõiguste alusdokumentidena saab nimetada inimõiguste ülddeklaratsiooni[15], inimõiguste ja põhivabaduste kaitse konventsiooni[16] (ka Euroopa inimõiguste konventsioon) ning kodaniku- ja poliitiliste õiguste rahvusvaheline pakti[17], mida aitab detailsemalt sisustada Euroopa Inimõiguste Kohtu ja Euroopa Kohtu praktika. Euroopa Liidus täidab põhiõiguste garanteerimise funktsiooni eelkõige Euroopa Liidu põhiõiguste harta[18], mille preambulist tulenevalt on üks keskseid põhimõtteid üksikisiku vabaduste väärtustamine ning isikuvabaduse ja -turvalisuse tagamine.

Samu väärtuseid kannab ka Euroopa Liidu õigus. Euroopa Liidu Toimimise Lepingu[19] (edaspidi ELTL) artikkel 3 punkti 2 kohaselt moodustatakse liit vabaduse, turvalisuse ja õigluse põhimõtetele tuginedes. Seda täiendavad ELTL artikkel 67 punktid 1 ja 3, mille kohaselt moodustatakse eelnimetatud põhimõtetel rajanev ala ning võetakse kasutusele meetmed turvalisuse taseme saavutamiseks. Samas on aga oluline märkida, et julgeoleku kaitsmine on ELTL artikkel 4 punkti 2 viimase lause kohaselt eelkõige iga liikmesriigi vastutada – konkreetset pädevust ei ole Euroopa Liidu aluslepingutega liidule antud. Avaliku korra tagamisel on Euroopa Liidu ja riikide rollide piir hägune: ELTL artikli 72 sõnastusega on jäetud lahtiseks Euroopa Liidu võimalus, sh ulatus valdkonda reguleerida. Euroopa Kohus on rõhutanud, et Euroopa Liidu põhiõiguste harta artikli 6 kohaselt on igaühel õigus isikuvabaduste kõrval ka turvalisusele.[20] Euroopa Kohus on erinevates lahendites tähtsustanud proportsionaalsuse printsiipi kui Euroopa Liidu õiguse üht põhiprintsiipi. Liikmesriikide

[14] R. Alexy. Põhiõigused Eesti põhiseaduses. – Juridica 2001/eriväljaanne, lk 5, 14.
[15] United Nations. The Universal Declaration of Human Rights. The UN General Assembly in Paris on 10th December 1948. – http://www.ohchr.org/EN/UDHR/Pages/UDHRIndex.aspx (22.12.2017).
[16] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57.
[17] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.
[18] Euroopa Liidu põhiõiguste harta. – ELT C 326, lk 391–407.
[19] Euroopa Liidu Toimimise Leping. – ELT C 83.
[20] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland*, p 42.

institutsioonide rakendatavad meetmed peavad olema eesmärgi saavutamiseks sobivad ja vajalikud ning erinevate meetmete valikuvõimaluse korral tuleb rakendada sellist meedet, mis on adressaadile võimalikult vähe koormav.[21] Siiski ei ole Euroopa Kohus ELTL artikkel 276 kohaselt pädev kontrollima liikmesriigi politsei või muu õiguskaitseorgani korraldatud operatsioonide põhjendatust või proportsionaalsust ega ka seda, kuidas liikmesriigid teostavad oma vastutust avaliku korra ja julgeoleku tagamisel. Samuti ei anna ELTL artikli 67 punkti 3 deklaratiivne olemus liikmesriikide kodanikele iseseisvat subjektiivset nõudeõigust.

Põhiseadusega tagatud põhiõigused on vastava riigivõimu jaoks siduvad. Nii on see ka Eesti põhiseaduse puhul – põhiõiguste tagamise kohustus kehtib Eesti riigivõimu jaoks universaalselt, olenemata olukorrast. Eraldi küsimus on, kas põhiõigused on siduvad ka eraisikute jaoks.[22] Käesolev analüüs antud probleemile tähelepanu ei pööra, vaid keskendub riigi kohustustele põhiõiguste ja -vabaduste tagamisel.

M. Ernits märgib, et riigi õiguskorras on põhiõiguste mõistet võimalik käsitada nii materiaalses kui formaalses tähenduses. Põhiõigused materiaalses tähenduses on riigi põhiõiguste hulka kuuluvad normid, mis olemuslikult omavad vähemalt osaliselt printsiibi tähendust. Põhiõigustena formaalses tähenduses käsitatakse käesolevas töös Eesti põhiseaduse teises peatükis sätestatud õiguseid. Neid täiendavad põhiseaduse teistes struktuuriosades paiknevad sätted, mis sisaldavad samuti erinevate õiguste määratlusi. Põhiõigusi defineeritakse ka kui üksikisikule kuuluvaid subjektiivseid õiguseid. Üldistades erinevate autorite lähenemisi subjektiivsetele õigustele, on M. Ernits märkinud, et ühelt poolt kohustab see riigivõimu teatud tegevusteks või tegevustest hoidumiseks, kuid laiemas tähenduses võib üksikisiku õiguseid tõlgendada ka õiguse instituudi või teatud eluvaldkonna vabaduse kontekstis.[23] Liberaalse konstitutsionalismiga riikides rakendatakse põhiõiguste kaitseks täidesaatva võimu laiendamisel konservatiivset lähenemist. Eelkõige puudutab see volitusi erakorralise situatsiooni lahendamisel, et vältida täidesaatva võimu otsuseid, millel on õiguskorda püsivalt muutev mõju.[24]

Põhiõiguse mõiste hõlmab Eesti õiguskorras sisuliselt ka põhivabaduse mõiste. Põhiõiguslikke vabadusi käsitatakse õiguslike negatiivsete tagatud vabadustena. Põhivabadust kui õiguslikku

[21] EKo 12.06.2001, C-189/01, *H.Jippes*, p 81.
[22] R. Alexy, lk 14.
[23] M. Ernits. Põhiõiguste mõiste ja tähtsus õigussüsteemis. – Juridica 1996/IX, lk 463–471.
[24] J. Ferejohn, P.Pasquino. The law of the exception: A typology of emergency powers. – Oxford University Press and New York University School of Law 2004, I.CON, Volume 2, Number 2, 2004, lk 210–211.

vabadust saab mõista kui võimalust mingisugust tegevusalternatiivi rakendada ja negatiivset vabadust kui kohustuse puudumist midagi teha või tegemata jätta. Vabaduse tagamisega on normi adressaadil selleks õigustatud luba.[25]

Põhiõiguste kaitse on Eesti õiguskorras tagatud põhiseadusega ehk teisisõnu on põhiõigustele antud põhiseaduslik jõud, mis kannab riigi olemuse ja toimimise fundamentaalset ideed. Üldjuhul on olulisimad riigi poolt kaitstavad õigushüved elu, tervis, vabadus, omand jmt. Põhiseaduse preambulis on rõhutatud sisemise ja välise rahu kaitse ülesannet ehk teisisõnu avalikku korda ja julgeolekut. Avalikku korda on põhiseaduses käsitatud õigushüvena, mille kaitseks võib teatud põhiõiguste[26] kasutamist legitiimselt piirata. Julgeolekut riigis võib käsitada kollektiivse õigushüvena, mis väljendub seisundis, milles riigi suveräänsus ja toimimine ei ole mõjutatud põhiseaduse vastaselt.[27] PS § 13 sätestab üldise kaitsepõhiõigusena igaühe õiguse riigi ja seaduse kaitsele, sealjuures on kodanikul õigus riigi kaitsele ka välisriikides. Sätte kolmandas lauses on seadusega ettenähtud kaitse riigi omavoli eest. Kuna tegemist on üldise normiga, siis praktikas täiendab seda riigi kohustus kaitsta teisi konkreetsemaid õigushüvesid. Sarnaselt muude õigusvaldkondadega kehtib põhiõiguste ja -vabaduste kaitse kohustus ka korrakaitseõiguses ja selle osana riikliku järelevalve teostamisel.

Oma kohustuste täitmiseks ja eesmärgi saavutamiseks on riigil õigus rakendada vajalikke meetmeid nii sooritusõigusena läbi õigusloome, õiguse rakendamise ja -mõistmise kui ka tõrjeõigusena, mis eeldab täidesaatva võimu poolt mingisuguse tagajärje ärahoidmiseks isikute põhiõigustesse sekkumist. Põhiõiguste kaitsmise peamine eesmärk on avaliku huvi tagamine, mistõttu ka isiku eraõiguslike huvide kaitsmine peab olema vastavuses avaliku huviga, et seda saaks käsitada põhiõigusliku hüve kaitsena. Just tõrjeõiguste puhul on oluline silmas pidada, et riigi sekkumine isikute põhiõigustesse oleks proportsionaalne saavutatava eesmärgiga ega muutuks ülemääraseks. Ka riikliku järelevalve läbiviimisel, millega sageli kaasneb riive, on oluline tagada isikute põhiõiguste ja -vabaduste kaitse.[28]

[25] M. Ernits, lk 463–471.
[26] Vt põhiseaduse järgmisi sätteid: §-s 26 teises lauses on sätestatud õigus piirata perekonna- ja eraelu puutumatust, § 33 teises lauses kodu puutumatust, § 40 lõikes 3 usutalituste täitmist, § 45 lõike 1 teises lauses informatsiooni levitamist, § 47 teises lauses kogunemis- ja koosolekuvabadust, § 130 esimeses lauses nimetatud tingimusel erakorralise või sõjaseisukorra ajal riigi julgeoleku või avaliku korra huvides.
[27] E. Kodar jt. PõhiS § 129/2 – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 4. täiend. vlj. Tallinn: Juura, 2017.
[28] J. Jäätma (viide 13), lk 35–38.

Eristatakse põhiõiguste ja -vabaduste isikulist ja esemelist kaitseala. Isikuline kaitseala määratleb subjektid, kellel on võimalik õigusele tugineda. Esemeline kaitseala tähendab konkreetset aspekti, mida põhiõiguste kaitsega tagatakse (kaitsehüve ehk põhiõiguslikult kaitstav hüve). Kaitse rakendumine on seotud asjaoluga, kas on toimunud kaitseala riive, mis teisisõnu on tinglikult riigipoolne ebasoodne mõju. Igasugune ebasoodne mõju pole ilmtingimata põhiõiguse rikkumine. Põhiõiguse riivest kujuneb rikkumine siis, kui avaldub selle formaalne või materiaalne õigusvastasus. Konkreetsed alused riive lubatavusele tulenevad põhiseaduses sätestatud nn piiriklauslitest. Lisaks tuleb arvestada, et kuigi põhiõiguste kaitsel peab riigivõim lähtuma nii individuaalsetest kui ka ühiskondlikest hüvedest, siis viimased ei ole alati taandatavad individuaalsete hüvede kogumiks.[29]

PS § 14 kohaselt on õiguste ja vabaduste tagamine seadusandliku, täidesaatva ja kohtuvõimu ning kohalike omavalitsuste kohustus. Norm täidab sisuliselt põhiõiguste garanteerimise funktsiooni riigi poolt – kaitset riigi omavoli vastu ja muude isikute õigusvastaste rünnakute eest kui ka riigi kohustust kohaldada asjakohaseid meetmeid, mis võimaldavad adressaatidel nende õiguste realiseerimist. Vastavad meetmed hõlmavad riigi organite süsteemi toimimist aga ka asjakohase menetlemise tagamist. Kokkuvõttes hõlmab PS § 14 erilist siduvust läbi kahe tähenduse: põhiõigused kui kaitse korraldusele ja menetlusele ning riigi kohustus vastavaid õiguseid tagada.[30] Ka ohutõrje ja riiklik järelevalve on üks osa riigi kohustuse täitmisest – nii vastava regulatsiooni kehtestamisena kui ka põhiseaduslike hüvede kõrval isiku individuaalsete õigushüvede kaitsmise tagamise korraldamisena.[31]

Põhiõiguste ja -vabaduste realiseerimise võimalus on PS § 15 kohaselt tagatud kohtu kaitsega. R. Alexy märgib, et põhiõigustel on demokraatlikes õigusriikides keskne roll ning see peegeldub ka Eesti põhiseaduses – ligi neljandik sellest ehk 48 paragrahvi on pühendatud põhiõigustele. Samuti toob ta välja, et põhiseaduses sisalduvad õigused on õiguslikult siduvad ning seetõttu ka tulenevalt PS § 3 lõike 1 esimesest lausest õigusemõistmisel kasutatavad.[32]

Põhiõiguste ja -vabaduste kaitse on seotud veel mitmete printsiipide rakendamisega. Võimude lahususe põhimõtte kohaselt täidavad nii seadusandlik, täidesaatev kui kohtuvõim neile määratud ja selgelt piiritletud ülesandeid. Riigikohus on märkinud, et põhiõigusi puudutavates küsimustes saab olulisi otsuseid langetada vaid seadusandja, täitevvõimul peab olema küsimuse

[29] R. Alexy, lk 34–35, 37–41.
[30] Sama, lk 9.
[31] J. Jäätma (viide 13), lk 39.
[32] R. Alexy, lk 5, 17.

lahendamiseks seaduslik alus. Parlamendireservatsiooni ehk olulisuse põhimõtte kohaselt ei saa täidesaatev võim otsustada küsimusi, mille lahendamise ainupädevus on seadusandjal. Samuti tuleb arvestada riive kaalu – nõude täitmist tuleb eriti jälgida, kui täitevvõimu tegevusega määratakse isikutele kohustusi või piiratakse nende õigusi.[33]

Põhiseadusest tuleneb ka seadusliku aluse nõue: PS § 3 lõike 1 esimese lause kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlaliste seaduste alusel ning PS § 11 esimese lause kohaselt tohib õigusi ja vabadusi piirata ainult kooskõlas põhiseadusega ega tohi moonutada piiratavate õiguste ja vabaduste olemust. PS § 13 lõike 2 kohaselt kaitseb seadus igaühte riigi omavoli eest. Seega kõik seadusliku aluseta põhiõiguste riived tuleb lugeda põhiseadusega vastuolus olevaks. Põhiõiguse riiveks peab olema nii formaalselt kui materiaalselt põhiseadusega kooskõlas olev alus. Materiaalse kooskõla all mõistetakse konkreetse normi olemasolu aga ka haldusorgani tegevuse vastavust nii õiguse üldpõhimõtetele kui ka kaalutlusreeglitele. Formaalne kooskõla tähendab, et põhiõigusi piirav õigustloov akt peab vastama põhiseaduses sätestatud pädevus-, menetlus- ja vorminõuetele ning olema kooskõlas määratletuse ja seadusereservatsiooni põhimõttega.[34] R. Alexy käsitluses on tegemist seadusreservatsiooni demokraatliku dimensiooniga.[35] Seadusliku aluse nõudega on seotud ka pädevusnormide ja volitusnormide eristamine. Kuna pädevusnormiga pannakse konkreetsele organile ülesandeid, siis sellega ei kaasne otseselt isiku õiguste riivet. Õiguseid ja kohustusi saab kehtestada volitusnormiga, mistõttu tuleb seadusandjal arvestada, et sellega kaasneb võimalik õiguste riive.[36]

Üks olulisemaid ja riivehalduses põhiseaduspärasuse hindamisel keskne põhimõte on proportsionaalsuse põhimõte ehk ülemäärasuse keeld, millega määratletakse põhiõiguste piiramise tingimused. PS § 11 teise lause kohaselt peavad õiguste ja vabaduste piirangud olema demokraatlikus ühiskonnas vajalikud. Nimetatud säte on ühtlasi proportsionaalsuse põhimõtte aluseks. PS § 11 esimeses ja teises lauses on kirjas kokku kolm eeldust, mis on põhiseaduslikkuse riives olulised: kooskõla põhiseadusega, vajalikkus demokraatlikus ühiskonnas ja keeld moonutada riivatavate õiguste ja vabaduste olemust. [37]

[33] RKHKo 3-4-1-10-2000, p 28.
[34] RKPJKo 3-4-1-5-05, p 7-8.
[35] R. Alexy, lk 36.
[36] RKÜKo 3-1-1-116-09, p 25.
[37] M. Ernits. PõhiS II peatüki sissejuhatus/54; M. Ernits. PõhiS § 11/1–2.

Riive proportsionaalsuse hindamisel on Riigikohus kasutanud kolmeastmelist testi, hinnates nimetatud järjekorras abinõu sobivust, vajalikkust ja mõõdukust ehk proportsionaalsust kitsamas tähenduses. Järjekord on põhjendatud asjaoluga, et abinõu ebasobivaks hindamise korral on tarbetu kontrollida proportsionaalsust järgmistel astmetel. Riigikohus on 2005. aastal märkinud ja mitmetes järgnevates lahendites korranud järgmist:
„Sobiv on abinõu, mis soodustab eesmärgi saavutamist. Vaieldamatult ebaproportsionaalne on sobivuse mõttes abinõu, mis ühelgi juhul ei soodusta eesmärgi saavutamist. Sobivuse nõude sisuks on kaitsta isikut avaliku võimu tarbetu sekkumise eest. Abinõu on vajalik, kui eesmärki ei ole võimalik saavutada mõne teise, kuid isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene. Arvestada tuleb ka seda, kuivõrd koormavad erinevad abinõud kolmandaid isikuid, samuti erinevusi riigi kulutustes. Abinõu mõõdukuse üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusse sekkumise ulatust ja intensiivsust, teiselt poolt aga eesmärgi tähtsust.“[38]

Seega kokkuvõttes on riigivõim kohustatud iga juhtumi lahendamisel oma otsuse aluseid kaaluma ja põhjendama. Sobivuse, vajalikkuse ja mõõdukuse kriteeriume on avatud täpsemalt järgmises alapeatükis.

1.2. Korrakaitseõigusel põhineva riikliku järelevalve olemus

1.2.1. Riikliku järelevalve ülesehitus

Riigi teostatavat järelevalvet reguleerivad Eestis mitmed aktid – kõige üldisemal tasandil põhiseadus ja sellega kooskõlas korrakaitseseadus kui korrakaitseõiguse üldosa, samuti valdkondlikud aktid. Riikliku järelevalve eesmärk on otseselt seotud riigi ja põhiseadusliku korra kaitsmise ülesande täitmisega. See järeldub ka põhiseaduse preambulist, mille kohaselt on rahvas kõrgema võimu kandjana näinud riigi ühe ülesandena sisemise rahu kindlustamise. Põhiseaduse kommentaarides on märgitud, et riigikaitse ei tähenda vaid riigi kaitsmist sõjalises mõttes, vaid on tänapäevases tähenduses oluliselt laiemalt sisustatav.[39] Riigikaitse laia käsitluse kohaselt kuulub siia alla kuus riigi kaitsega seotud valdkonda: sõjaline kaitse, tsiviilsektori toetus sõjalisele kaitsele, rahvusvaheline tegevus, siseturvalisuse tagamine, elutähtsate teenuste toimepidevuse kindlustamine ja psühholoogiline kaitse, hõlmates seega lisaks sõjalistele meetmetele ka mittesõjalisi meetmeid.[40] Sisejulgeoleku (siseturvalisuse) tagamist loetakse riigi

[38] RKPJKo 3-4-1-1-02, p 15.
[39] E. Kodar jt. PõhiS X peatüki sissejuhatus/3.
[40] Eesti Vabariigi Kaitseministeerium. „Riigikaitse arengukava 2013 – 2022 mittesõjalised osad" avalik kokkuvõte. Sissejuhatus. – http://www.kaitseministeerium.ee/riigikaitse2022/laiapohjaline-riigikaitse/index.html (21.04.2018).

esmaseks ja ühtlasi võõrandamatuks ülesandeks – sisuliselt nii riigi õiguseks kui ka kohustuseks. Ka Riigikohus on sisustanud põhiseaduse preambulist tulenevat sisemise julgeoleku ja rahu tagamise eesmärki kollektiivse hüvena ja suure kaaluga õigusväärtusena, mille tagamiseks on põhiõiguste piiramine legitiimne.[41]

Valdkondlikus kirjanduses kasutatakse nii sisejulgeoleku kui siseturvalisuse mõisteid, kuid nende eristamise osas pole ühtset lähenemist. Eesti õigekeelsussõnaraamat nimetab turvalisuse ja julgeoleku sünonüümidena.[42] Näiteks Siseministeerium on sisemise julgeoleku alavaldkondadena toonud välja põhiseadusliku korra ja riigisaladuse kaitse, terrorismi- ja korruptsioonivastase võitluse ja küberjulgeoleku.[43] Kübervaldkonna strateegiadokumentides on kasutatud nii küberturvalisuse kui -julgeoleku mõisteid, kuid alati ei ole neid sisuliselt eristatud.[44] Sarnaselt ei ole käesolevas töös julgeoleku ja turvalisuse mõisteid sisuliselt eristatud. Kuna turvalisus on korrakaitse valdkonna loogikale omasem mõiste, siis on käesolevas töös kasutatud eelkõige sise- ja küberturvalisuse mõisteid, kus see on asjakohane.

Siseturvalisuse tagamine hõlmab erinevaid valdkondi, muuhulgas nii politsei kui paljude teiste korrakaitseorganite tegevusvaldkondi, mida tervikuna mõistetakse korrakaitsena. Ka riigi poolt läbiviidav järelevalve on osa korrakaitsest, olles haldusmenetluse eriliik. Riikliku järelevalve kõrval eksisteerivad eraldi liikidena teenistuslik ja haldusjärelevalve. Lisaks kasutatakse siseturvalisuse tagamisel kaht eraldi menetluse liiki: riikliku järelevalve kõrval ka süüteomenetlust, mis on sarnase eesmärgiga.[45] Võrreldes nimetatud menetlusliike omavahel, on mõlemad suunatud õigushüvede kaitsmisele ja riigi toimimise tagamisele laiemalt, kuid nende meetmed ja tagajärjed on erinevad. Erinevalt karistusõigusest ei saa riikliku järelevalve sisu olla suunatud karistamisele, vaid õigusliku kahjustuse ennetamisele või selle vähendamisele.[46] Ka Riigikohus on rõhutanud vajadust kaht menetlusliiki eristada, hoolimata sellest, et seadusandja pole vastavaid tingimusi selgelt määratlenud ja puudub püsiv kohtupraktika. Eristamisest olenevad muuhulgas menetluse korraldus, läbiviiva ametniku pädevuse piirid jm asjaolud.[47] Käesolevas töös süüteomenetlusega seotud küsimusi lähemalt ei käsitleta.

[41] RKPJKo 3-4-1-2-01, p 15.
[42] Eesti õigekeelsussõnaraamat: ÕS 2013. – Tallinn: Eesti Keele Sihtasutus 2013, lk 975.
[43] Eesti Vabariigi Siseministeerium. Siseministeeriumi eesmärk ja tegevused, sisejulgeoleku tagamine. – https://www.siseministeerium.ee/et/siseturvalisuse-valdkond/sisejulgeoleku-tagamine (21.04.2018).
[44] Vt mõistete selgitusi Küberjulgeoleku strateegia 2014–2017 lisas 2 (viide 1).
[45] Korrakaitseseaduse eelnõu seletuskiri. 49 SE I, lk 9, 13–14. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4/Korrakaitseseadus (21.04.2018).
[46] J. Jäätma (viide 13), lk 11–12, 19.
[47] RKÜKo 3-3-1-75-11, p 15.

Eestis on loodud korrakaitseseadusega ühtne raamistik kogu riiklikule järelevalvele. Seadusandja on korrakaitseseaduses lähtunud ohutõrje kontseptsioonist. Teisisõnu on riikliku järelevalve sisu meie õiguskorras ohu ennetamise ja tõrjumise keskne. KorS § 2 lõike 4 kohaselt on riikliku järelevalve eesmärk ennetada ohtu, selgitada see välja ja tõrjuda või kõrvaldada korrarikkumine. Ohu ennetamisena saab mõista mingisuguse tegevuse või tagajärje ärahoidmist, tõkestamist.[48] Sealjuures korrakaitseorganid ei saa oma pädevust korrakaitseseadusest, vaid organi tegevust reguleerivast seadusest. Korrakaitseseadus täpsustab vaid organi korrakaitselisi ülesandeid.[49]

Korrakaitseseadus on võrdlemisi uus – seadus võeti vastu 2011. aastal ning jõustus 2014. aastal – ja selle rakenduspraktikat on kujunenud vaid mõne aasta jooksul. Eelnõu seletuskirjas kirjeldatud seadusandja kavatsuse kohaselt võeti korrakaitseseaduse kehtestamisega eesmärgid määratleda avalik kord, oht ja muud kesksed mõisted, samuti korraldada ohtude ennetamine, tõrjumine ja kõrvaldamine läbi korrakaitseorganite süsteemi ja üksikisikute ning kokkuvõttes määratleda tervikuna riikliku järelevalve alused.[50] Samuti väärib märkimist, et korrakaitseseadusega reguleeriti korrakaitse valdkond Eesti õiguskorra jaoks täiesti uue kontseptsiooni kohaselt. Näiteks Riigikohus on eelkirjeldatud ohutõrje keskset lähenemist hinnanud Eesti õigusele võõraks ning ebaotstarbekaks. Sobivamaks lahenduseks on peetud üldosas inspektsioonilise järelevalve ning sellega seotud menetluslike normide reguleerimist ning eriseadustes konkreetse valdkonna pädevus- ja volitusnormide andmist.[51] Antud hinnangust saab järeldada, et Riigikohus ei toetanud seadusandja püüet korrakaitseseadusega suurt osa riikliku järelevalve meetmetest ühtlustada. Samas on tulenevalt praktilisest vajadusest meetmeid täpsustatud mitmetes eriseadustes, mida Riigikohus oma arvamuses märkis.

Valdkondliku alusaktina sisaldab korrakaitseseadus nii üld- kui erimeetmeid, eriseadused vaid erimeetmeid. Üld- ja erimeetme kohaldamise õiguse suhtes saab tuua analoogia üld- ja erinormi kohaldamisega. Erinorm on üldnormi suhtes ülimuslik ning üldnorm tuleb üldjuhul kohaldamisele juhul, kui olukorra lahendamiseks puudub vastav erinorm. Üldnorm täidab seega n-ö lüngatäite funktsiooni, kuna seadusandja ei ole võimeline ette nägema ja spetsiaalselt reguleerima kõiki võimalikke olukordi, näiteks ebatüüpilisi situatsioone või uusi ohte, mistõttu

[48] Eesti õigekeelsussõnaraamat: ÕS 2013, lk 147.
[49] M. Laaring, lk 79.
[50] Korrakaitseseaduse eelnõu seletuskiri, lk 1.
[51] Eesti Vabariigi Riigikohus. Arvamus korrakaitseseaduse muutmise ja rakendamise seaduse eelnõu (424 SE) kohta, p 5.1–5.5. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/arvamused/2445bcfe-b04d-40c8-932e-db51253abea3/Korrakaitseseaduse%20muutmise%20ja%20rakendamise%20seadus (21.04.2018).

ohutõrje efektiivsuse saavutamiseks ei ole võimalik sedalaadi normidest loobuda.[52] Korrakaitseorganile antud üldvolitus lubab avaliku korra kaitseks sekkuda, kui esineb konkreetne oht.[53] Vajadus riikliku järelevalve erimeetmete kehtestamiseks valdkondlikes seadustes tekib eelkõige konkreetse valdkonna spetsiifikast tulenevalt. Sageli jääb üldnorm õigussuhete korraldamisel liiga üldsõnaliseks ja olukorra lahendamiseks on vaja detailsemat normi. Vastavaid norme on võimalik anda eriseadustega, sealhulgas neid võrreldes üldseadusega kitsendada või laiendada ulatuse, sisu, suuna ja mahu või ka kaalumisruumi poolest.[54] Üks selliseid näiteid on ka koostamisel olev küberturvalisuse seaduse eelnõu[55], millega RIA-le kavandatakse anda õigused riikliku järelevalve erimeetmete rakendamiseks.

Riigi tegevus korrakaitseõiguse rakendamisel on sisuliselt jagatav kaheks: ohtude ennetamine kui eelfaas ja realiseerunud ohtude põhjustatud tagajärgedega tegelemine kui põhifaas. Sisuliselt on tegemist tõrjeõiguste ja kaitseõiguste realiseerimisega. Tõrjeõigus on seotud isiku õigusega olla puutumata riigi negatiivsest sekkumisest, sh et riik ei takistaks isikul tema õiguseid ellu viimast ja selleks konkreetseid tegevusi tegemast jms. Ohutõrjeõigusega on loodud materiaalõiguslik alus, mis võimaldab isikute põhiõigusi ja -vabadusi piirata ehk sisuliselt luuakse alused riive lubatavusele, kasutades selleks volitus- ja pädevusnorme. Omakorda eristatakse ohtude tõrjumist ohtude ennetamisest – kui tõrjevajaduse puhul on ilmnenud reaalne oht, mille mõjusid asutakse vähendama, siis ennetusfaasi puhul saame rääkida ohu võimalikkusest.[56]

Ohutõrjeõigus peab olema suunav, toetav ja ennetusliku loomuga aga ka ühiskondlikke vajadusi arvestav. Eesmärk on aidata läbi ohtude tõrjumise kaasa siseturvalisuse tagamisele, kaitstes sellega inimeste turvalisust kui põhiseaduslikku järku väärtust, samuti muid õigushüvesid kahjustamise eest.[57] Põhiseaduse kommentaarides leiti, et ohutõrjes rakendatavad riikliku järelevalve meetmed on tavapäraselt isikute põhiõiguseid ja -vabadusi riivavad. Siiski tuleb arvestada, et siseturvalisuse tagamise eesmärgi kõrval on riigil kohustus garanteerida ka põhiõiguste kaitse. Antud juhul on riigi kohustuste väljendus korrakaitseseaduse kui korrakaitse üldosa kehtestamine, riigi ülesannete täitmise eest vastutavate korrakaitseorganite ringi määratlemine ja menetlusreeglite kehtestamine. Iga riigi poolt planeeritava meetme puhul on oluline hinnata selle kooskõla põhiseaduslike alustega – see saab tuleneda vastavasisulise

[52] F. Schoch, M. Ernits. Üldklausli vältimatus nüüdisaegses ohutõrjeõiguses.– Juridica 2010/VIII, lk 545–546.
[53] I. Pärnamägi. Avaliku korra mõiste Eesti ohutõrjeõiguses. – Juridica 2016/IV, lk 242.
[54] F. Schoch, M. Ernits, lk 541-542; J. Jäätma (viide 13), lk 79–80, 106.
[55] Vt viide 4.
[56] R. Alexy, lk 8–9, 22–25.
[57] J. Jäätma. The Constitutional Requirements for Averting of a Danger. – Juridica International 2012/XIX, lk 137.

põhiseaduse normi puudumisel põhiseaduse preambulist või läbi konkreetsete põhiõiguste ja -vabaduste, mis otseselt reguleerivad nende piiramise võimalusi tulenevalt avaliku korra tagamise kaalutlustest.[58] Samas tuleb arvestada, et tegemist on tasakaalu otsimisega erinevate huvide vahel. Ühiskondlikus kooselus pole võimalik lõputult luua ja realiseerida isiku vabadusi selleks teise isiku õiguseid piiramata. Riigi rollina on siinkohal käsitletav nii konfliktide ennetamine kui ka lahendamine.

Ohukoosseisu sisu järgi eristatakse kaht riikliku järelevalve meetmete gruppi: konkreetse ohu kahtluse, ohu ja korrarikkumise korral rakendatavaid meetmeid ning meetmeid, mida rakendatakse konkreetsest ohust sõltumata. KorS § 2 lõike 4 kohaselt piiritletakse riiklikku järelevalvet kui korrakaitseorgani tegevust eesmärgiga ennetada ohtu, selgitada see välja ja tõrjuda või kõrvaldada korrarikkumine. Nimetatud elemendid kokku moodustavad korrakaitseõiguse keskse idee. KorS § 5 lõike 7 kohaselt käsitatakse ohu ennetamisena osa korrakaitsest, kus puudub ohukahtlus, kuid ühtlasi saab pidada võimalikuks olukorda, mille realiseerumisel tekib ohukahtlus või oht. Ohu ennetamine on muu hulgas teabe kogumine, vahetamine ja analüüs, toimingute kavandamine ja elluviimine ning riikliku järelevalve meetmete kohaldamine avalikku korda tulevikus ähvardada võivate ohtude tõrjumiseks, sealhulgas süütegude ennetamine. Sisuliselt eristatakse ohu ennetamist ohukahtlusest, ohutõrjumisest, avalikku korda ähvardava ohu väljaselgitamisest ja korrarikkumise kõrvaldamisest. Vastavalt on korrakaitseorganil võimalik valida ka kohaldatavaid meetmeid tuginedes KorS § 5 lõigetes 2–6 defineeritud ohutasemetele.

Konkreetse ohukahtluse puudumisel saab korrakaitseõiguse kohaselt järelevalve olla inspektsiooniline. Iga järelevalvemeetme kohaldamine eeldab, et korrakaitseorganil on selleks volitused. Võrreldes ohutõrjelise järelevalvega peab isikute õigustesse ja vabadustesse sekkumine olema inspektsioonilise järelevalve puhul piiratum. Ühtlasi peavad vastavad meetmed olema enam põhjendatud ja selgelt proportsionaalsed saavutatava eesmärgiga. Alles inspektsioonilise järelevalve käigus tuvastatud konkreetse ohu või ohukahtluse tulemusena muutub see ohutõrjeliseks järelevalveks. Eelkõige on tuvastatud oht või konkreetne ohukahtlus korrakaitseorgani jaoks isikute põhiõiguste piiramist õigustav asjaolu. Isikute põhiõiguste riive ohtu ennetavate või väljaselgitavate meetmete rakendamisel on põhjendatud vaid väga väärtuslike hüvede kaitseks või valdkonnas, mille eripära õigustab rangemaid nõudeid.[59]

[58] M. Ernits, N.Parrest. PõhiS § 14/9–16.
[59] Korrakaitseseaduse eelnõu seletuskiri, lk 47–48.

1.2.2. Riikliku järelevalve meetme kohaldamine ja proportsionaalsuse põhimõte

Riikliku järelevalve meetmete kohaldamisel tuleb lähtuda korrakaitseseaduse kolmanda peatüki esimeses jaos sätestatud üldpõhimõtetest. Reeglina on võimalik korrakaitseseaduses sätestatud meetmeid kohaldada vaid avaliku korra ees vastutava ehk ohu tekitanud isiku suhtes või selles kahtlustatava isiku suhtes, kui seaduses ei ole teisiti ette nähtud (KorS § 23 lg 1). Siiski on erandina osa meetmeid võimalik rakendada ka isiku suhtes, keda korrakaitseorgan ei pea avaliku korra tagamise eest vastutavaks – sellised on KorS § 23 lõike 2 kohaselt teavitamine, küsitlemine ja dokumentide nõudmine, isikusamasuse tuvastamine jm nimetatud meetmed. Seaduse alusel ja õiguspäraselt kohaldatavaid korrakaitsemeetmeid on subjektil kohustus taluda ning selle tagamiseks saab riikliku järelevalve organ vajadusel kasutada ettekirjutust ning rakendada sunniraha (KorS § 23 lg-d 3 ja 4).

Korrakaitseõiguses on oluline riivevolituse seisukohast teha vahet meetmetel, mis on suunatud ohu ennetamiseks (puudub konkreetne ohukahtlus, oht või korrarikkumine) ja ohu tõrjumiseks (rakendatakse konkreetse ohu kahtluse, ohu või korrarikkumise korral). KorS §-s 27 on sätestatud, et ohukahtluse korral on pädeval korrakaitseorganil õigus kohaldada seaduses ettenähtud meetmeid ohu olemasolu väljaselgitamiseks. Kuna korrakaitseseadus sisaldab vaid üksikuid ohu ennetamisel rakendatavaid meetmeid, siis on seadusandja jätnud KorS § 1 lõikega 3 võimaluse eriseadustega luua volitusnormid, mille alusel erikorrakaitseorganitel on võimalik kohaldada konkreetse ohukahtluse puudumisel inspektsioonilisi riikliku järelevalve meetmeid. Tegemist on seega viitelise normiga, mis osundab abstraktselt meetmete rakendamise võimalikele alustele. Inspektsiooniline järelevalve võib muutuda menetluse käigus korrakaitseorgani poolt konkreetse ohu või ohukahtluse tuvastamisel ohutõrjeliseks järelevalveks. Sellisel juhul muutub ka rakendatavate meetmete valik. Lisaks võib konkreetses olukorras lubatavate meetmete valik olla kehtestatud Euroopa Liidu määrusega, mis on otsekohalduv.[60]

KorS § 24 lõigete 1 ja 3 kohaselt võib ohu ennetamiseks riikliku järelevalve erimeedet kohaldada tulenevalt ohuprognoosist, sealjuures ulatuses, mis on vajalik konkreetsel juhul ja kehtivast õigusest tulenevate nõuete täitmise tagamiseks. Antavast hinnangust peab selguma ohu realiseerumise võimalikkus, mis tugineb sama paragrahvi lõike 2 kohaselt faktidele või teadmispõhisele infole. Ohu ennetamise faasis ei ole reeglina lubatud kohaldada vahetut sundi, välja arvatud olulise või kõrgendatud ohu korral. Samuti pole lubatud ohu ennetamiseks

[60] Sama, lk 48.

kohaldada sundtoomist, kui isik jätab kutse peale kohale ilmumata (KorS § 24 lg 6). Siiski on KorS §-ga 25 reguleeritud võimalus kohaldada riikliku järelevalve meetmeid ohu väljaselgitamiseks, kui selleks on valdkonna eest vastutava ministri luba.

Korrakaitseorgan on rakendatava riikliku järelevalve meetme valikul seotud haldusmenetluse seaduse[61] (edaspidi HMS) § 4 lõikest 2 tuleneva proportsionaalsuse nõudega – seda eelkõige põhjusel, et riive aluseks olevad õigusnormid on sõnastatud üldiselt.[62] Haldusõiguses eristatakse kahte liiki kaalutlust: otsustuskaalutlus ja valikukaalutlus. See kehtib ka korrakaitseõiguses, sh riikliku järelevalve teostamisel. Otsustuskaalutluse puhul on kaalutlusõigust omaval organil õigus valida, kas konkreetses küsimuses on vaja otsus langetada või valida erinevate alternatiivide vahel, kui need on olemas. Valikukaalutluse korral on organil õigus valida meede, teha otsustus selle rakendamise ja rakendamise objekti kohta.

Seadusandja jätab nimetatud kahe kaalumisviisi kaudu täidesaatvale organile võimaluse haldusmenetluses ja selle eriliigina riikliku järelevalve menetluses kaaluda erinevaid aspekte ning langetada olusid arvestades kõige optimaalsem otsus. Esmalt hinnatakse, kas haldusorgani tegevus oli formaalselt õiguspärane. Seejärel hinnatakse materiaalse õiguspärasuse raames, kas valitud abinõu oli sobiv, vajalik ja mõõdukas. Ebaproportsionaalse abinõu rakendamisel ilmneb vastuolu põhiseadusega ning tegemist on materiaalselt õigusvastase tegevusega. Sobivuse ja vajalikkuse nõuded kui proportsionaalsuse testi esimene ja teine aste sisalduvad korrakaitseseaduses ühes sättes: § 7 lõike 1 järgi kohaldab korrakaitseorgan riiklikku järelevalvet teostades mitmest sobivast ja vajalikust riikliku järelevalve meetmest seda, mis nii isikut kui ka üldsust eeldatavalt kõige vähem kahjustab.[63]

Korrakaitseseaduse eelnõu seletuskirja kohaselt tähendab riikliku järelevalve meetme sobivus, et oht on võimalik kiirelt ja lõplikult korrakaitseorgani tegevusega kõrvaldada. Mitme sobiva meetme korral tuleb valida meede, mis oma olemuselt nii üksikisiku kui üldsuse huve tervikuna vähim kahjustab. Vajalikkus kui nn leebeima vahendi põhimõte tähendab, et mitme võrdselt sobiva meetme vahel valides tuleb eelistada isikut ja üldsust võimalikult vähe koormavat varianti. Meede peab aitama eesmärki saavutada ning sealjuures koormama üksikisikut põhiõiguste kandjana kõige vähemal määral.[64] Proportsionaalsuse testi kolmas aste ehk mõõdukuse nõue on korrakaitseseaduses selgemalt sõnastatud: § 7 p 2 kohaselt on haldusorgan

[61] Haldusmenetluse seadus. – RT I, 25.10.2016, 5.
[62] RKHKo 3-3-1-80-11, p 11, 16.
[63] R. Alexy, lk 43–44.
[64] Korrakaitseseaduse eelnõu seletuskiri, lk 29–30.

kohustatud kohaldama meedet, mis on proportsionaalne eesmärgiga, mida sellega taotletakse. Meetme eesmärgi puhul tuleb hinnata ka selle kaalu – tugevama riive korral peab eesmärk olema suurema kaaluga. Samuti on korrakaitseseaduse eelnõu seletuskirja kohaselt oluline ajaline mõõde – vajaduse äralangemine või võimatus eesmärki saavutada loetakse ebaproportsionaalseks.[65] Kokkuvõtlikult tuleb haldusorganil leida konkreetset olukorda arvestades asjakaohane meede, mis võimaldab saavutada eesmärgi koormates isikut vähimal võimalikul määral.

Van Kempen on märkinud, et turvalisus ja julgeolek ning inimõiguste ja -vabaduste kaitse pole ilmtingimata vastandlikud eesmärgid. Kuigi probleemi võib näha eelkõige esimese põlvkonna inimõiguste ehk kodaniku- ja poliitiliste õiguste tagamise ning julgeoleku paradigmade vahel, on nende eesmärgid omavahel tihedalt seotud ja teineteist täiendavad. Ka inimõiguste tagamine peaks kaasa aitama turvalisuse kasvule, kuid olukorra muudab keeruliseks asjaolu, et pole üheselt mõistetav, mida tähendab turvalisus inimõiguste tagamise seisukohast.[66] Sarnane probleem ilmneb ka küberruumis turvalisuse ning põhiõiguste ja -vabaduste tagamise vahel tasakaalu otsimisel.

[65] Sama, lk 30.
[66] P.H. van Kempen. Four concepts of security. A human rights perspective. – Human Rights Law Review, March 2013, 13(1), lk 3, 7.

2. KÜBERRUUMIS TURVALISUSE TAGAMINE JA ÕIGUSLIK REGULEERIMINE

2.1. Turvalisust ohustavad suundumused küberruumis ja levinumad küberintsidendi liigid

Enne õiguslike küsimuste juurde siirdumist on käesolevas alapeatükis käsitletud turvalisust ohustavaid suundumusi[67] küberruumis, samuti on antud ülevaade enim esinevatest küberintsidendi liikidest. Küberintsidente ehk arvutivõrgus toimunud kahjuliku mõjuga sündmuseid on võimalik klassifitseerida mitmel alusel, näiteks rünnaku või kaitsetegevuse omaduste, samuti rünnaku mõju põhjal.[68] Käesolevas töös on lähtutud RIA jt organisatsioonide avalikku kasutusse antud informatsioonist ega ole kasutatud konkreetset küberintsidentide liigitamise alust. Eesmärk on informatsiooni põhjal hinnata, milliste probleemide lahendamisele aitab riigi sekkumine kaasa riikliku järelevalve kaudu.

ÜRO küberturvalisuse valitsusekspertide grupp on koostanud kolm küberturvalisuse konsensusraportit – 2010., 2013. ja 2015. aastal (edaspidi: *ÜRO raport(id)*). Need toovad esile info- ja kommunikatsioonitehnoloogiaga seonduvate probleemide üldise olemuse. Koos info- ja kommunikatsioonitehnoloogia kasutusulatuse laienemisega on kaasnevad riskid ajas suurenenud ja muutunud – iga andmevõrguga ühendatud tehniline vahend kujutab endast hüpoteetiliselt väärkasutuse sihtmärki. Küberruum on pahatahtliku tegevuse jaoks atraktiivne globaalse ühenduse, tehnoloogiate haavatavuse ja anonüümsuse tõttu. Mobiilsete seadmete, veebiteenuste, sotsiaalvõrgustike ja pilvandmetöötluse laialdane levik muudavad nende kasutamise turvalise tagamise järjest suuremaks väljakutseks. Laiaulatusliku kahju tekitamine on küberruumis võrdlemisi lihtne, samas kui selle eest vastutava isiku kindlakstegemine ja karistamine on keeruline. Lisaks on infosüsteemide kaudu kuritegude toimepanemine või vastase ründamine võimalik väga kiiresti, hoolimata suurtest vahemaadest.[69] Eelnimetatud

[67] Vt küberjulgeoleku strateegia 2014–2017 (viide 122). Strateegias kasutatakse küberturvalisust ohustavate arengute kohta üldistavalt suundumused, sama on autor teinud käesolevas töös. Kuigi ÜRO raportites, Eesti ametkondade koostatud aastaraamatutes jm kasutatakse mõistet oht, tekitaks selle kasutamine antud kontekstis segadust, kuna korrakaitseõiguses on oht teistsuguse tähendusega.

[68] W.B. Miller. Classifying and Cataloging Cyber-Security Indidents Within Cyber-Physical Systems. Brigham Young University, 2014, lk 3–4. – https://scholarsarchive.byu.edu/etd/4345 (21.04.2018).

[69] United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201). United Nations General Assembly, 2010, lk 6-7. – https://undocs.org/A/65/201 (21.04.2018); United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98*). United Nations General Assembly, 2013, lk 6-8. – https://undocs.org/A/68/98 (21.04.2018); United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). United Nations General Assembly, 2015, lk 6-7. – https://undocs.org/A/70/174 (21.04.2018).

probleemid kujutavad ka Eesti jaoks riske, kuid suure üldistusastme tõttu ei ole nende puhul silmas peetud ohte korrakaitseseaduse mõistes. Täiendavat õiguslikku probleemi võib kujutada ka kübertegevuse eristamine avaliku korra tagamise ja sõjalises tähenduses riigikaitse seisukohast, mille suhtes kohaldatakse erinevat õigust. Sõjalise riigikaitse küsimusi käesolevas töös lähemalt ei käsitleta.

Erinevate motiividega kurjategijad, terroristid jt ohustavad küberruumi kaudu riikide aga ka rahvusvahelist julgeolekut tervikuna. Kuigi ründe toimepanija on indiviid või grupp, võib vastav tegevus olla algatatud ja toetatud mõne riigi poolt. Vastutuse omistamine konkreetsele riigile on enamasti keeruline, mistõttu selles eksimine võib viia riikidevahelise konfliktini. Ka arendavad mitmed riigid info- ja kommunikatsioonitehnoloogiaid luure- ja sõjapidamisvahenditena, mida võib käsitada küberrelvadena. Samas on riikide võimekus enda kaitseks küberruumis erinev, mis avaldab mõju kogu küberruumi turvalisusele. Küberruum pakub ka terroristlikel eesmärkidel efektiivseid võimalusi informatsiooni kogumiseks, liikmete värbamiseks, ideede levitamiseks aga ka rünnakute planeerimiseks ja koordineerimiseks.[70]

Ühiskonna toimimise jaoks hädavajalike teenuste ja infrastruktuuri puhul on kujunenud probleemiks sõltuvus info- ja kommunikatsioonitehnoloogiast. Eestis nimetatakse selliseid teenuseid koos vajaliku infrastruktuuriga elutähtsateks teenusteks (HOS § 2 lg 4). Siia hulka kuuluvad näiteks elekter, kaugküte, vedelkütus, veevarustus, side, vältimatu arstiabi, mis moodustavad teenuste vundamendi, milleta ei saa ühiskond meile harjumuspäraselt toimida.[71] Elutähtsate teenuste sõltuvus info- ja kommunikatsioonitehnoloogiast muudab need rünnakute suhtes haavatavamaks, mis omakorda suurendab võimalust sattuda tegeliku rünnaku alla, kuna mõju saavutamine osutub ründajale lihtsaks.[72] Eestis sõltub ligi viiendik elutähtsate teenuste osutajatest kriitilisel määral kolmandate isikute pakutavatest teenustest, mistõttu oluline risk on küberintsidendi tulemusena elutähtsate teenuste toimepidevuse katkestuste tekkimine. Samuti nähakse probleemina teenuseosutajate vahelisi ristsõltuvusi, mille tõttu katkestus ühe teenusepakkuja juures mõjutab ka teisi. Eelkõige puudutab see valdkondi, mille puhul katkestuse mõju ühiskonnale on suur – näiteks energeetika, tervishoiu-, finantsteenused jm. Enim on nimetatutest puudutatud Eesti tervishoiusektor. Seetõttu võimaliku küberintsidendi korral on ohustatud näiteks vältimatu abi osutamine.[73]

[70] Sama.
[71] Eesti Vabariigi Siseministeerium. Elutähtsad teenused. – https://www.siseministeerium.ee/et/eesmark-tegevused/kriisireguleerimine/elutahtsad-teenused (21.04.2018).
[72] United Nations, 2010, lk 6–7 ja 2013, lk 6–8.
[73] Eesti Vabariigi Riigi Infosüsteemi Amet. Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2015. aasta kokkuvõte, lk 5-6. – https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html (21.04.2018).

Üldjoontes toovad RIA küberturvalisuse teenistuse ja Kaitsepolitseiameti (edaspidi KAPO) ülevaated välja samad probleemid, mis ÜRO raportid. KAPO 2016. aasta aastaraamat jagab küberturvalisusega seotud ohuallikad kolmeks: küberluure, sabotaaž ja mõjutustegevus küberruumis.[74] Eesti eripära seisneb selles, et riigi ja ühiskonna toimimine on tugevalt seotud e-teenuste toimimisega, mistõttu nii juhuslikud kui sihistatud kübertegevused kujutavad järjest kasvavat ohuallikat. Lisaks eelnimetatutele tuleb arvestada Venemaa agressiivse käitumisega ja küberründevõime jätkuva arendamisega. Välisluureamet näeb Eesti jaoks suurima ohuna just Venemaa algatatud küberrünnakuid.[75] Kuivõrd rünnakute tegelikke algatajaid ja eesmärke on keeruline kindlaks teha, on problemaatiline ka õigeaegsete ja asjakohaste järelduste tegemine. KAPO 2015. aasta aastaraamatus märgitakse, et Eestile ja teistele siinse regiooni riikidele kujutab riski kübersabotaažiga võrgu- ja infosüsteemide töö kahjustamine.[76]

RIA märgib ühe ohuallikana Eesti küberturvalisusele ka infosüsteemide kasutajate tegevust. Peamised põhjused seisnevad inimeste oskamatuses või puudulikus teadlikkuses turvanõuetest ja vastavate riskide maandamisest. Näiteks kasutatakse aegunud arvutitarkvara, mille puhul ei ole turvariske kõrvaldatud. Uut tüüpi ohuallikat kujutab endast laieneva kasutusalaga nn asjade interneti ehk esemevõrgu haavatavus. Kuivõrd igapäevakasutuses olevad seadmed muutuvad järjest nutikamaks ning info- ja kommunikatsioonitehnoloogia kasutusala laieneb, muutub järjest suuremaks probleemiks sellega seotud riskide haldamine ja turvalisuse tagamine.[77]

Asetleidnud küberintsidentide liikide osas toob Euroopa Liidu Võrgu- ja Infoturbeamet (edaspidi ENISA) 2016. aasta näitel välja peamise ja kasvava intsidendiliigina pahavara, sh lunavara levitamise ja teabevargused. Tavapärased on ka interneti kaudu toimepandud ründed: veebilehtede ja veebirakenduste, sh veebilehitsejate laienduste kaudu ründamine aga ka teenustõkestus- ja robotvõrku hõivamise ründed. Teiste levinumate intsidendiliikidena märgitakse teabeõngitsemine, spämmimine, samuti kasutajast ja füüsilisest tegevusest tulenevad probleemid (n. tundmatu andmekandja ühendamine võrgusüsteemiga), andmetega manipuleerimine, identiteedivargused, infolekked ja küberspionaaž. Sageli kombineerivad ründajad erinevaid ründeviise, samuti võidakse kasutada valitud ründeviisi muu tegevuse

[74] Eesti Vabariigi Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2016, lk 20. – https://kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html (21.04.2018)
[75] Eesti Vabariigi Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2017, lk 36. – https://www.valisluureamet.ee/hinnang.html (21.04.2018).
[76] Eesti Vabariigi Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2015, lk 22. – https://kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html (21.04.2018)
[77] Küberturvalisuse teenistuse 2015. aasta kokkuvõte, lk 5-6.

varjamiseks.[78] RIA 2016. aasta ülevaate kohaselt moodustasid valdava osa Eestis registreeritud küberintsidentidest e-kirjade ja veebilehtede kaudu pahavara levitamine, samuti kasutaja teadmata ülevõetud arvutitega ehk robotvõrku hõivamisega seotud juhtumid. Viimast viisi kasutatakse sageli ka koordineeritud küberrünnakute läbiviimisel. Muud levinud intsidendiliigid olid infoõngitsused ja lunavara levitamine (mõlemal juhul ohvrilt proovitakse saada kätte eelkõige raha või tundlikke andmeid), serverite hõivamine, veebilehtede näotustamine ning hajusad teenustõkestusründed (*DDoS* ründed).[79]

Eelnevat ülevaadet üldistades võivad erinevad küberintsidendi liigid olla seotud erinevate küberruumi turvalisust ohustavate suundumustega. Olukorra näitlikustamisel on abiks järgnev kaasus. 2017. aasta mais levis üle maailma suuremahuline lunavara rünnak WannaCry (ka WanaCypt0r jt nimede all). Lunavara krüpteeris ohvri arvutis olevad failid ning nende dekrütpeerimiseks nõudsid kurjategijad bitcoinides umbes 300–600 euro suurust makset. Nakatunud arvutitest levis lunavara automaatselt edasi, kasutades ära Windows operatsioonisüsteemi teatud haavatavust, mida olemasoleva turvauuenduse paigaldamisega arvutis ei olnud kõrvaldatud. Sama haavatavust oli enne rünnakut väidetavalt luureoperatsioonidel kasutanud Ameerika Ühendriikide Riiklik Julgeolekuagentuur, mille kohta lekitasid infot häkkerid. Mitukümmend suurfirmat ja erinevate riikide haldusorganit teatasid oma arvutisüsteemide nakatumisest rünnaku tagajärjel, näiteks rahvusvaheline logistikafirma FedEx, Hispaania telekomiettevõte Telefonica ja Suurbritannia haigekassa. Rünnakus nakatus kokku hinnanguliselt 200 000 arvutit 150 riigis, sh Eestis. Siiski osutusid mõjud kokkuvõttes suhteliselt tagasihoidlikuks, kuna lunavara levikule suudeti kiiresti piir panna, kui avastati, kuidas selle saab n-ö välja lülitada. Samuti polnud sihtmärgiks otseselt kriitilise infrastruktuuri objektid.[80] Kui ettevõtete puhul on kahju tõenäoliselt majanduslik, siis tervishoiusektoris lunavaraga arvutisüsteemide töö blokeerimine mõjutab suure tõenäosusega inimeste elu ja tervist. Antud näitel valmistas andmete krüpteerimine probleeme, kuna selle tulemusena muutusid Suurbritannias patsiendiandmed ligipääsetamatuks. Paljusid meditsiiniseadmeid juhivad tänapäeval aga võrguühendusega arvutid, mistõttu nende töö katkemisel on võimalik tagajärg juba ravivajavate inimeste hukkumine.[81]

---

[78] European Union Agency for Network and Information Security. ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends, lk 21-65, 74. – https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (21.04.2018).
[79] Küberturvalisuse teenistuse 2016. aasta kokkuvõte, lk 6-12.
[80] H. Lõugas. Üle maailma levis reedel suur krüptolunavara laine. – https://geenius.ee/uudis/ule-maailma-levib-suur-kruptolunavara-laine/ (21.04.2018); Wikipedia. WannaCry ransomware attack. – https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (21.04.2018).
[81] Vt näiteks 13. mail 2017 Eesti Päevalehes ilmunud RIA peadirektori asetäitja arvamusartiklit. – http://epl.delfi.ee/news/arvamus/ria-peadirektori-asetaitja-toomas-vaks-kuberrunnak-seab-ohtu-inimeste-elud?id=78203446 (21.04.2018).

2.2. Korrakaitseõiguse kohaldamine küberturvalisuse tagamisel

2.2.1. Korrakaitseõiguse kesksed mõisted ja nende seos küberturvalisuse valdkonnaga

Enne sisu juurde siirdumist on asjakohane avada korrakaitseõiguse ja küberturvalisuse valdkonna mõistete seoseid, kuna nende kasutamisel on mõningad erisused. Ohu kui korrakaitseõiguse ühe keskse mõiste sätestab KorS § 5 lõige 2: oht on olukord, kus ilmnenud asjaoludele antava objektiivse hinnangu põhjal võib pidada piisavalt tõenäoliseks, et lähitulevikus leiab aset korrarikkumine. Korrakaitseseaduse eelnõu seletuskirjas on märgitud, et seadusandja on ohuna mõistnud konkreetset olukorda ehk mingisuguses elulises situatsioonis ilmnevat ohtu, mitte abstraktset teadmist selle esinemise võimalikkusest. Sealjuures tuleb lähtuda nn mõistliku korrakaitseametniku vaatepunktist, rakendades olukorra hindamisel sotsiaalseid ja ametialaseid teadmisi ning kogemusi. Ohu kindlakstegemisel hinnatakse objektiivselt avaliku korra rikkumise asetleidmise võimalikkust lähitulevikus. Selleks peab olema piisav tõenäosus, arvestades ohustatud hüve tähtsust ja ohutõrjel kasutatavate meetmete põhiõiguste riive ulatust. Vastava tõenäosuse puudumisel võib olla tegemist ohukahtlusega, mille puhul ei saa rääkida kindlakstehtud ohust. Siis on tegemist ohu kindlakstegemise eelse etapiga, kuna pole piisavalt andmeid, et ohu olemasolu tuvastada.[82] Ka Riigikohus on märkinud, et ohu puhul on tegemist olukorraga, kus on põhjust karta õigushüve olulist kahjustumist, olenemata selle päritolust.[83]

Infotehnoloogia valdkonnas on oht defineeritud ISO standardis, mille kohaselt on oht arvutiturvalisuse võimalik rikkumine.[84] Küberintsidendi puhul on aset leidnud aga konkreetne arvutiturvalisuse rikkumine. Võrgu- ja infosüsteemide turvalisuse direktiiv[85] (edaspidi NIS direktiiv) defineerib küberintsidenti kui sündmust, mis tegelikult kahjustab võrgu- ja infosüsteemide turvalisust. Samuti on küberintsidenti defineeritud kui arvutivõrgu kasutamisel tekitatud sündmust, millega kaasneb kahjulik toime infosüsteemile või selles sisalduvale teabele.[86] Küberturvalisuse seaduse eelnõus, millega võetakse eelnimetatud direktiiv Eesti õigusesse üle, käsitatakse küberintsidendina samuti võrgu- ja infosüsteemis toimuvat sündmust, mis kahjustab süsteemi turvalisust (KüTS eelnõu § 2 p 4).

[82] Korrakaitseseaduse eelnõu seletuskiri, lk 22–24.
[83] RKKKo 3-1-1-95-06, p 12.
[84] International Organization for Standardization. ISO/IEC 2382:2015. Information technology – Vocabulary. Märksõna *threat*. – https://www.iso.org/standard/63598.html (21.04.2018).
[85] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. – ELT L 194, lk 1–30.
[86] Cybernetica AS. Andmekaitse ja infoturbe leksikon. Märksõna *cyber incident* – http://akit.cyber.ee/term/1187-cyber-incident#t_1187 (21.04.2018).

Ohu kõrgemad tasemed on määratletud KorS § 5 lõigetega 3–5: oluline, kõrgendatud ja vahetu oht. Olulise ohu puhul on seadusandja näinud sisuliselt vaheastet tavapärase ohutaseme ja kõrgendatud ohu vahel, puudutades isiku tervist, olulise väärtusega varalist hüve, keskkonda või teatud süütegude toimepanemise tõenäosust.[87] Kõrgendatud ohuna määratleb KorS § 5 lõige 4 ohtu isiku elule, kehalisele puutumatusele, füüsilisele vabadusele, suure väärtusega varalisele hüvele, suure keskkonnakahju tekkimise ohtu ja samuti teatud raskemate süütegude toimepanemise ohtu. Vahetu ohu puhul on KorS § 5 lõike 5 kohaselt korrarikkumine juba alanud või selle realiseerumise võimalikkus on lähitulevikus suur. Küberturvalisuse seaduse eelnõus selliselt ohutasemeid ei eristata. Küll aga kasutatakse mõistet olulise mõjuga küberintsident, jättes avamata selle sisu ja seosed korrakaitseseaduse tähenduses ohu või selle kõrgemate tasemetega. Eelnõu § 8 lõike 6 kohaselt kehtestab olulise mõjuga küberintsidendi kriteeriumid Vabariigi Valitsus. Seletuskirjas on toodud vastavate näidetena teenuse osutamise häiritus või takistus teenustõkestusründe mõjul.[88] NIS direktiivi artikkel 6 lõikes 1 on sätestatud olulise häiriva mõjuga intsidendi määramiseks vähemalt kuus tegurit, sh intsidendi võimalik mõju avalikule julgeolekule.

Korrakaitseõiguse ja riikliku järelevalve meetmete rakendamisel on keskseid mõisteid ka avalik kord.[89] Põhiseadus mõiste sisu täpsemalt ei ava, kuid see on sisustatud korrakaitseõiguses. KorS § 4 lõike 1 tähenduses on tegemist ühiskonna seisundiga, milles on tagatud õigusnormide järgimine ning õigushüvede ja isikute subjektiivsete õiguste kaitstus. Seletuskirja kohaselt on tegemist elukorraldusega, mis tugineb õigusnormidele, sisaldades muuhulgas isikute õiguste ja vabaduste kaitset ja turvalisuse tagamist. Avalik kord hõlmab lisaks avalikus kohas kehtivatele reeglitele ka kõiki muid elualasid, seda kitsalt ruumiliselt piiritlemata. Teisisõnu, termin peegeldab avalikes huvides kaitstavat õiguskorra osa, laienedes kõikidele elualadele.[90] Sisuliselt võib välja tuua kolme liiki kaitsehüvesid, mida avalik kord sisaldab: õigusnormide järgimine, õigushüvede ja subjektiivsete õiguste kaitse. Avaliku korra tagamise alla kuulub ka põhiõiguste ja -vabaduste kaitse.[91]

Seadusandja on avaliku korra ja avaliku koha (KorS § 54) mõisted määratlenud võrdlemisi abstraktselt. Avalikku kohta saab käsitada kui kõigile inimestele ligipääsetavat ala või ruumi ning seal käitumiseks on sätestatud korrakaitseseaduses üldnõuded (KorS § 55). Küberruum on

[87] Korrakaitseseaduse eelnõu seletuskiri, lk 23.
[88] Küberturvalisuse seaduse eelnõu seletuskiri (kuupäevaga 03.10.2017 ametlikule kooskõlastamisele esitatud versioon). – https://eelnoud.valitsus.ee/main/mount/docList/e7ff643b-8b72-4a70-8f3e-dab03f9ca79f (21.04.2018), lk 15.
[89] Vt ka I. Pärnamägi käsitlust avaliku korra mõistest (viide 53).
[90] Korrakaitseseaduse eelnõu seletuskiri, lk 19.
[91] I. Pärnamägi, lk 246.

aga virtuaalne võrgustik ehk mõtteline keskkond, milles tegevus toimub omavahel ühenduses olevate arvutite jm seadmete ning seda võimaldava infrastruktuuri abil.[92] Siiski on vähe arutletud teemal, kas ja millises ulatuses on küberruum avalik koht ning kohalduvad avalikus kohas käitumise üldnõuded. Üks võimalik tõlgendus on, et küberruum on avalik koht ja avaliku korra tagamine puudutab ka küberruumis toimuvat. Küberruum on lahutamatult seotud internetiga, mis ühendab arvutiseadmeid üle maailma. Seega vähemalt osaliselt on küberruumi käsitamine avaliku kohana põhjendatud, kuid sellel on omad piirid, kuna kõik interneti vahendusel toimuvad tegevused ei ole avalikud.[93] Käsitades küberruumi avaliku kohana, kujuneb ruumi ulatus antud valdkonnas sisuliselt hoomamatuks. Kuid arvestades, et avaliku korra tagamine ei piirdu vaid avalikus kohas korra tagamisega, siis ei mõjuta antud küsimus otseselt korrakaitseõiguse kohaldamise võimalikkust küberturvalisuse tagamise eesmärgil.

Ohu ja avaliku korra mõisted on omakorda seotud korrarikkumise mõistega. Korrarikkumisena käsitatakse KorS § 5 lõike 1 kohaselt avaliku korra kaitsealas oleva õigusnormi või isiku subjektiivse õiguse rikkumist või õigushüve kahjustamist. Sealjuures on avaliku korra rikkumisega tegu ka juhul, kui kahjustatakse kellegi õigushüve, mis on õiguskorraga kaitstud.[94] Turvalisust võib seega käsitada kui kaitstust riskide realiseerumise eest. Kuigi küberturvalisus on õigusmõistena määratlemata, on seda sisustatud kehtiva küberjulgeoleku strateegia lisas 2, mis on koos põhidokumendiga kinnitatud Vabariigi Valitsuse korraldusega. Väljapakutud selgituse sisu on autori hinnangul praktilise kasutuse jaoks siiski liiga abstraktne ja selle ühene mõistetavus kaheldav: küberturvalisus hõlmab kübervahendite turvalisuse kui ka turvalisuse kübervahendite talitluse kaudu avalduvate ohtude suhtes. Kübervahend on samas defineeritud kui infotöötlusvahend, mis on võimeline vastastikku suhtlema teiste infotöötlusvahenditega.[95] Teiste riikide praktika näitab, et küberturvalisust on võimalik defineerida erinevatel viisidel, sealjuures varieerub kõnesolev sisu ja ulatus võrdlemisi laias ulatuses.[96]

Samuti vajab lahendamist küsimus, kas küberintsident on käsitatav korrarikkumisena. Kuigi küberruumi meeleliselt tajutav olemus avaldub infotehnoloogiliste vahendite ja infrastruktuuri kaudu, võivad küberintsidendi mõjud avalduda füüsilises maailmas. Küberruumis toimepandud

[92] Vt mõiste selgitust Eesti õigekeelsussõnaraamat: ÕS 2013, lk 92: avalik on kõigile mõeldud või ette nähtud, kõikide kasutada olev. Küberruumi mõistet ja selle kujunemist on avatud Wikipedia artiklis, mis on leitav aadressil https://et.wikipedia.org/wiki/K%C3%BCberruum (21.04.2018). Vt ka Küberjulgeoleku strateegia 2014–2017 lisa 2 (viide 1).
[93] Vt näiteks J. Camp, Y.T. Chien. The Internet as Public Space: Concepts, Issues, and Implications in Public Policy.– John F. Kennedy School of Government. Harvard University. Avaldatud uudiskirjas ACM SIGCAS Computers and Society. Volume 30 Issue 3, September 2000.
[94] I. Pärnamägi, lk 248.
[95] Küberjulgeoleku strateegia 2014–2017 lisa 2, lk 4, 6 (04.01.2018).
[96] Vt teiste riikide definitsioonide näiteid NATO küberkaitsekoostöö keskuse kodulehel https://ccdcoe.org/cyber-definitions.html (21.04.2018).

teod võivad avaldada väga erinevat mõju, sh võivad need olla käsitatavad süütegudena ja raskemal juhul ohustada inimese elu või tervist, varalist hüve või põhjustada keskkonnakahju. Oht ja ohu kõrgendatud tasemed korrakaitseõiguse mõistetena on kohaldatavad ka küberruumis. Seega võib asuda seisukohale, et korrarikkumise tunnuste olemasolul on küberintsident käsitatav korrarikkumisena.

Mõistete kasutuse juures väärib veel märkimist, et küberturvalisuse analüüsides kirjeldatakse lisaks valdkondlikele ohtudele ka riske. Korrakaitseseadus riski mõistet ei sisalda, aga KorS § 7 lõige 6 defineerib ohukahtluse kui ebapiisava tõenäosuse korrarikkumise asetleidmiseks olukorras, kus puudub alus ka seda välistada. Eelnimetatud ISO standardi kohaselt mõistetakse riskina võimalust, et mingisugune konkreetne oht kasutab ära andmetöötlussüsteemi haavatavust.[97] Käesolevas analüüsis on kasutatud nii ohu kui riski mõistet, lähtudes konkreetse allika sõnastusest. Autor ei eristanud neid sisu poolest, kuna selleks puudus antud kontekstis otsene vajadus.

2.2.2. Korrakaitseõiguse kohaldamise piirid

Küberruumis valitsevate suundumuste põhjal on järgmise sammuna hinnatud, milliste probleemide lahendamisel ja millises ulatuses saab korrakaitseõigust kohaldada. Analüüsis ei käsitleta detailsemalt rahvusvahelise õiguse reguleerimisalasse jäävaid küsimusi. Koondülevaade küberturvalisust ohustavate suundumuste ja kohalduva õiguse seostest on vormistatud tabelina (vt tabelit lisas).

Eelmises alapeatükis käsitletud levinumate küberintsidentide liikide – pahavara levitamine, seadme robotvõrku hõivamine, infoõngitsus, lunavara levitamine, serveri hõivamine, veebilehe näotustamine ja hajus teenustõkestusrünne – puhul on tahtlus suunatud ebaseadusliku kasu saamisele või kellegi kahjustamisele, mistõttu saab neid käsitleda süütegudena. Küberruumis toimepandud süüteod võivad osutuda nii riigisiseseks kui ka riikide piire ületavaks probleemiks. Piiriülese küberkuritegevuse vastu võitlemisel kohaldatakse rahvusvahelistest lepingutest tulenevat õigust – Eesti on ühinenud näiteks arvutikuritegevusevastase konventsiooniga[98]. Riigi vastutusalasse jääb oma territooriumil õiguskorra tagamine. Seega kui kübertegevus ohustab kedagi riigi territooriumil ja on objektiivse õiguskorraga vastuolus, kahjustades seeläbi avalikku huvi üldiselt, kuulub küsimus avaliku korra tagamise kaitsealasse

[97] International Organization for Standardization. ISO/IEC 2382:2015. Märksõna *risk*.
[98] Arvutikuritegevusvastane konventsioon. – RT II 2003, 9, 32.

ning vastava tegevuse peatamiseks on alust rakendada korrakaitseõigust. KüTS eelnõu § 17 lõike 1 kohaselt ja lõikes 2 toodud kumulatiivsete piirangutega kooskõlas võib riikliku järelevalve teostamisel RIA võtta üle küberintsidendi tõkestamiseks võrgu- ja infosüsteemi juhtimise ning piirata küberintsidendist põhjustatud kõrgendatud ohu väljaselgitamiseks või tõrjumiseks süsteemi kasutamist või sellele juurdepääsu. Seega on küberturvalisuse seaduse eelnõus olemas õiguslik alus küberintsidendist tuleneva ohu korral kiireloomuliseks reageerivaks tegevuseks. Oluline on sealjuures eristada ohu tõrjumiseks suunatud riiklikku järelevalvet süütegude menetlemisest, mille eesmärk on toimepanijat karistada. Kuritegude toimepanemise karistamist küberruumis reguleerib karistusõigus ja vastavad alused on sätestatud karistusseadustikus. KarS §-de 206, 207, 213, 216[1] ja 217 alusel on karistatavad vastavalt arvutiandmetesse sekkumine, arvutisüsteemi toimimise takistamine, arvutikelmus, arvutikuriteo ettevalmistamine ja arvutisüsteemile ebaseaduslikult juurdepääsu hankimine. KarS §-ga 207 on kriminaliseeritud muuhulgas teenustõkestusründed.[99] Siiski pole karistusseadustikus reguleeritud süüteokoosseisude sõnastuses selgelt viidatud konkreetsetele küberintsidendi liikidele. Kuna tegemist on teise astme kuritegudega KarS § 4 lõike 3 kohaselt, siis taoliste sisuga küberintsidentide puhul võib avalduda oluline oht KorS § 5 lõike 3 tähenduses. Eelkõige võib see avalduda vara kahjustamisena aga ka inimeste elude ohustamisena, nagu ilmes eelkäsitletud WannaCry lunavara rünnaku näite puhul.

Küberturvalisuse seaduse eelnõu kohaselt on lubatud lisaks ohule reageerimisele ka küberintsidendi ohu korral ennetavalt tegutseda – KüTS eelnõu § 13 lõigete 2 ja 3 kohaselt kuulub RIA ülesannete hulka küberintsidentide ennetamiseks olukorra seire, süsteemide turvalisust ohustavate riskide mõju analüüs ja ohuteadete edastamine. Seega küberkuritegevuse kontekstis on ohtude ennetamiseks ja neile reageerimiseks korrakaitseõiguse keskne lähenemine üldjoontes sobiv.

Kübertegevus võib olla seotud terrorikuriteo või selle ettevalmistamisega, olles ohuks nii riigi kui rahvusvahelisele julgeolekule. Eesti õiguse kohaselt on vastavad teod karistatavad KarS §-de 237 ja 237[2] alusel. Mõlema puhul on tegemist esimese astme kuriteoga KarS § 4 lõike 2 tähenduses. Sarnaselt küberkuritegevusele tuleb arvuti vahendusel sooritatud terroristlikku tegevust käsitada avaliku korra vastase tegevusena. Olenevalt olukorrast võib oht olla nii oluline kui kõrgendatud KorS § 5 lõigete 3 ja 4 tähenduses, näiteks kui kavandatakse inimeste pihta suunatud rünnakuid avalikes kohtades. Kuivõrd võrgu- ja infosüsteemid võivad osutuda

[99] E. Hirsnik. Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid. – Juridica 2014/VIII, lk 617.

terroristidele vahendiks vajaliku info kogumisel, liikmete värbamisel, ideede levitamisel, rünnakute planeerimisel ja koordineerimisel jm tegevustel, on oluline taoline tegevus vajadusel kiiresti peatada, enne kui terroristide tegevus kujuneb otseseks ohuks inimeste elule ja tervisele. Terrorismivastane võitlus on laiaulatuslik tegevus ja küberruumi vahendusel teostatavad tegevused on tervikust vaid üks osa. Riikliku järelevalve tegevustel võib terrorismi tõkestamisel olla oma roll ka küberturvalisuse valdkonnas.

Olenevalt olukorrast võib elutähtsate teenuste katkemisest tulenev oht olla nii oluline kui kõrgendatud KorS § 5 lõigete 3 ja 4 tähenduses. Näiteks võib selline olukord olla ulatusliku elektrikatkestuse põhjustamine, mille tulemusena on igapäevaelu oluliselt häiritud. Samuti on riigivalitsemine seotud erinevate teenuste ja digitaalsete süsteemidega, mis omakorda sõltub vastavast infrastruktuurist. Elutähtis ehk kriitiline infrastruktuur on Euroopa Liidu õiguse kohaselt vara, süsteem või nende osa, mis on hädavajalik eluliselt tähtsateks ühiskondlikeks toiminguteks.[100] Elutähtsast infrastruktuurist osa moodustab kriitilise informatsiooni infrastruktuur, mis hõlmab riigi toimimise jaoks olulisi võrgu- ja infosüsteeme.[101] Süsteemide toimepidevuse tagamiseks tuleb määrata nende olulisus ja korraldada kaitse, milleks kohustab Euroopa Liit elutähtsate infrastruktuuride identifitseerimise, määramise ja kaitsmise direktiiv[102] ja riigisisene õigus. Kuna kaitse korraldamine on peaasjalikult teenuse osutaja ülesanne, siis HOS § 38 lõike 3 punktis 1 on ette nähtud elutähtsa teenuse osutajale kohustus koostada enda osutatava elutähtsa teenuse toimepidevuse riskianalüüs ja plaan tuvastatud riskide maandamiseks. Samuti on eriolukorras HOS § 33 lõigete 1 ja 2 alusel õigus eriolukorra väljakuulutamise põhjustanud hädaolukorra lahendamiseks kohustada elutähtsa teenuse osutajat vastava teenuse osutamiseks ja ka kohustada piirama lõppkasutajate võimalust teenust või sidevõrku kasutada. Küberturvalisuse tagamiseks on teenuse osutajal kohustus rakendada alaliselt organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid (KüTS eelnõu § 7 lõige 1).

Küberturvalisust ohustava suundumusena käsitatakse ka spionaaži. Eesti õigusruumis ei ole spionaaž õigusterminina kasutusel. Lihtsustatult on küberspionaaži ehk -luure puhul tegemist piiratud ligipääsuga informatsiooni kogumisega, kasutades selleks info- ja kommunikatsioonitehnoloogiaid. Alternatiivselt on võimalik luuret teostada ka avalikke

[100] Nõukogu direktiiv 2008/114/EÜ, 8. detsember 2008, Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta, artikkel 2 p a. – ELT L 345, lk 75–82.
[101] Eesti Vabariigi Riigi Infosüsteemi Amet. Kriitilise informatsiooni infrastruktuuri kaitse. – https://www.ria.ee/ee/kiik.html (21.04.2018).
[102] Nõukogu direktiiv 2008/114/EÜ, 8. detsember 2008, Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta. – ELT L 345, lk 75–82.

andmeallikaid[103] kasutades. *Tallinn Manual*-is märgitakse, et luuretegevust riikide vahel ei loeta jõu kasutamiseks, seega pole tegevus otseselt keelatud. Küll aga tuleb eristada lubatud ja lubamatuid meetodeid.[104] Eestis reguleerib luuretegevuse põhialuseid julgeolekuasutuste seadus[105] ja sõjalise luure osas kaitseväe korralduse seadus[106]. Korrakaitseõiguse kontekstis kujutab küberspionaaž ohtu ka (intellektuaalse) omandi puutumatusele. Näiteks on võimalik, et tööstusettevõtte infosüsteemi tungimise eesmärk on ligipääs ärisaladusele. Tööstusomand on Eestis kaitstav tööstusomandi õiguskorralduse aluste seadusega.[107] Tõenäoliselt võib tööstusspionaaži korral olla tegemist olulise või kõrgendatud ohuga KorS § 5 lõike 3 või 4 tähenduses, kui tegevus toob kaasa olulise või suure väärtusega varalise hüve kahjustamise näiteks olukorras, kus saadud teavet müüakse kuritegelikul eesmärgil või kasutatakse riigikorra destabiliseerimiseks. Kui spioneerimine avaldub riigivastase tegevusena, siis on tegemist kõrgendatud ohuga KorS § 5 lõike 4 tähenduses, kuna küberspionaaži mõjud võivad olla kaugeleulatuvad muuhulgas riigikorra destabiliseerimisel.

Võrgu- ja infosüsteemide kasutajate tegevusest tulenev oht küberturvalisusele on aktuaalne nii üksikisikute, organisatsioonide kui ka riigi tasandil. Kuna põhjused on vähene turvateadlikkus, aegunud tarkvara kasutamine jms, siis pole otstarbekas probleemi lahendada vaid regulatsiooni kehtestamisega. Vähene turvateadlikkus üksinda ilma teise isiku pahatahtliku tegevuseta turvalisust otseselt ei ohusta. Seega saab asuda seisukohale, et tegemist pole korrakaitseseaduse mõistes ohuga, vaid ohukahtlusega KorS § 5 lõike 6 tähenduses. Riigi jaoks oluliste infosüsteemide toimimiseks on kehtestatud turvameetmete süsteemi (ISKE)[108] rakendamise kohustus. Täiendav lahendus turvanõuete kõrval on ka jätkuv kasutajate teadlikkuse tõstmine koolituste ja teavitamise vormis nende tegevusega kaasnevatest riskidest, riskide realiseerumise tagajärgedest ja turvameetmetest. RIA on vastavaid meetmeid seni rakendanud, sh pakkunud avalikke koolitusi küberturvalisuse alase teadlikkuse tõstmiseks.[109]

Võrgu- ja infosüsteemide ja nendega seotud seadmete kasutajatele on kahtlemata oluline usaldusväärsus ja ohutus. Küberturvalisuse seaduse eelnõus on reguleeritud teenuse osutaja, digitaalse teenuse osutaja ning riigi ja kohaliku omavalitsuse üksuse süsteemi turvanõuded. Lisaks inimkäitumisega seotud riskidele tuleb aga arvestada, et võrgu- ja infosüsteemide kaudu

[103] Vt näiteks Wikipedia artiklit teemal *Open Source Intelligence*. – https://en.wikipedia.org/wiki/Open-source_intelligence (21.04.2018).
[104] Schmitt, M.N. (gen.ed.), lk 168-175.
[105] Julgeolekuasutuste seadus. – RT I, 05.05.2017, 2.
[106] Kaitseväe korralduse seadus. – RT I, 05.05.2017, 3.
[107] Tööstusomandi õiguskorralduse aluste seadus. – RT I, 28.12.2011, 46.
[108] Infosüsteemide turvameetmete süsteem. VVm 20.12.2007 nr 252. – RT I 2009, 6, 39.
[109] Vt näiteks Riigi Infosüsteemi Ameti koolituste kalender. – https://www.ria.ee/ee/koolitused.html (21.04.2018).

on ühendatud järjest rohkem seadmeid, mida on samuti võimalik programmeerida kahju tekitama. Näiteks on võimalik interneti-ühendusega seadet hõivata robotvõrku ja kasutada seda elutähtsa teenuse osutaja infosüsteemi ründamiseks. Usaldusväärsuse ja ohutuse puhul ei saa siiski rääkida ohust korrakaitseõiguse mõistes. Kasutatava tehnoloogia ja osutatava teenuse turvalisusele saab riik kehtestada nõudeid, kuid säilib võimalus, et kõiki võimalikke probleeme ei ole võimalik ette näha.

Lisaks käsitletud kübertegevuste vormidele eristatakse ka küberründeid. Tegemist on määratlemata õigusmõistega, mis on küberintsidendist erinev, kuid sellega seotud mõiste.[110] Roscini märgib, et üks olulisimaid aspekte rünnaku tuvastamisel on hinnata, kas kübertegevuse puhul on jõutud jõu kasutamise tasemeni – vastasel juhul on tegemist muu ebaseadusliku kübertegevuse vormiga, mitte küberründega.[111] Küberründega seotud õiguslikke küsimusi reguleerib rahvusvaheline õigus.

Kokkuvõttes saab välja tuua, et korrakaitseõigusel põhinev reguleerimine puudutab vaid osa küberturvalisust ohustavatest suundumustest. Probleemide lahendamisele aitavad kaasa ka mitmed muud meetmed peale järelevalve – eelkõige andmekaitse- ja infoturbemeetmete aga ka mitteregulatiivsete meetmete rakendamine, näiteks koolitamine. Käsitletud suundumuste kontekstis on riikliku järelevalve meetmed küberturvalisuse tagamisel kohased esmajoones küberkuritegevuse vastase võitluse ja elutähtsate teenuste toimepidevuse tagamise eesmärgil. Lisaks on need rakendatavad ka teatud osas terrorismi ning küberspionaaži vastase võitluse eesmärgil. Oluline on, et rakendatavad riikliku järelevalve meetmed oleksid sidustatud küberturvalisust ohustavate suundumustega, kuid need peavad ühtlasi olema proportsionaalsed taotletava eesmärgiga.

[110] Vt üht võimalikku käsitlust Küberjulgeoleku strateegia 2014–2017 lisas 2, lk 6 (viide 1).
[111] M. Roscini. Cyber operations and the use of force in international law. Oxford University Press, 2014, lk 43-45.

3. RIIKLIK JÄRELEVALVE KÜBERTURVALISUSE VALDKONNAS

3.1. Riigi Infosüsteemi Ameti riikliku järelevalve teostamise õiguslikud alused ja meetmete proportsionaalsus

RIA ülesanded ehk tema pädevus on reguleeritud asutuse põhimääruses[112] ja valdkonnapõhiselt mitmes seaduses. Põhimääruse § 7 kohaselt teostab RIA õigusaktidega sätestatud ulatuses riigi poliitika ja arengukavade elluviimist ning täidab avalikke ülesandeid riigi infosüsteemi, elektroonilise identiteedi tarkvara, usaldusteenuste, küberturvalisuse ja kriitilise informatsiooni infrastruktuuri kaitse valdkonnas. Ametile on põhimääruse §-ga 8 määratud kokku 11 põhiülesannet, mille hulka kuulub ka punkti 1 kohaselt haldus- ja riikliku järelevalve teostamine ameti tegevusvaldkondi reguleerivate õigusaktide nõuete täitmise üle ja nende nõuete rikkumise korral riikliku sunni rakendamine. Põhiülesannete täitmiseks käsitleb RIA turvaintsidente, mis toimuvad Eesti arvutivõrkudes, koostab nendest raporteid, annab ennetava sisuga hoiatusi ja tegeleb üldise turvateadlikkuse tõstmisega (RIA põhimäärus § 9 p 3), teostab küberturbe seiret (RIA põhimäärus § 9 p 4^1) ja korraldab kriitilise informatsiooni infrastruktuuri kaitset (RIA põhimäärus § 9 p 1), teostab järelevalvet elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete alalise rakendamise üle (RIA põhimäärus § 9 p 5), samuti infosüsteemide turvameetmete süsteemi rakendamise ja vastava andmevahetuskihiga liitumise (RIA põhimäärus § 9 p 7), sidevõrkude ja -teenuste turvalisuse ja terviklikkuse tagamise (RIA põhimäärus § 9 p 7^1) üle ning täidab muid talle määratud ülesandeid. Kuigi RIA ülesannete hulka kuulub ka haldusjärelevalve teostamine, siis käesolevas analüüsis haldusjärelevalve meetmetel pikemalt ei peatuta, vaid fookuse hoidmise eesmärgil keskendutakse riikliku järelevalve meetmetele.

RIA teostatav riiklik järelevalve võrgu- ja infosüsteemide turvalisuse üle on reguleeritud mitmes seaduses, puudutades seni vaid teatud valdkondi. ESS § 133 lõike 5 kohaselt on RIA ülesanne riikliku järelevalve teostamine sidevõrkude ja -teenuste turvalisuse ning terviklikkuse tagamise, sideettevõtja kaabellevi- või ringhäälinguvõrgu teenuse elektroonilise turvalisuse, kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse elektroonilise turvalisuse tagamise üle. Avaliku teabe seaduse[113] (edaspidi AvTS) § 53^1 lõige 1 sätestab sarnaselt RIA põhimäärusele, et asutus teostab järelevalvet infosüsteemide turvameetmete süsteemi rakendamise ja vastava andmevahetuskihiga liitumise üle ning nimetab lõikes 2

[112] Riigi Infosüsteemi Ameti põhimäärus. MKMm 25.04.2011 nr 28. – RT I, 29.12.2016, 14.
[113] Avaliku teabe seadus. – RT I, 06.01.2016, 7.

kohaldatavad riikliku järelevalve erimeetmed. HOS § 45 lõige 1 kätkeb endas pädevusnormi elutähtsa teenuse osutamise elektroonilise turvalisuse tagamise üle. Lisaks on RIA teostatavat järelevalvet reguleeritud ka mere-, raudtee- ja õhuveo valdkondades. Vastavalt sadamaseaduse[114] § 42 lõige 5, raudteeseaduse[115] § 71 lõige 7^1 ja lennundusseaduse[116] § 60^1 lõige 5 viitavad sarnases sõnastuses HOS regulatsioonile elutähtsa teenuse osutamise elektroonilisele turvalisusele kehtestatud nõuete täitmise üle kontrolli teostamiseks.

Eelnevates õigusanalüüsides on küberturvalisuse valdkonda reguleerivate aktidega seonduvalt välja toodud erinevaid probleeme.[117] Muuhulgas on advokaadibüroo LEXTAL koostatud analüüsis jõutud järeldusele, et RIA korrakaitse alased ülesanded on peamiselt ennetuslikud ega võimalda täita ülesandeid küberturvalisuse tagamiseks vajalikus ulatuses.[118] Õigusselguse suurendamiseks näeb RIA vajadust õigusliku kehtestada killustatuse vähendamiseks seadusjõuga akti tasandil terviklik regulatsioon, kuidas riik küberintsidentidele reageerib.[119] Seni kehtivas õiguses nimetab ESS vaid sideettevõtja kohustused RIA-t intsidendist teavitada, vajadusel avalikkust teavitada ja esitada RIA-le hinnangu andmiseks nõutud teavet sideettevõtja poolt turvalisuse tagamiseks võetud meetmete kohta ning ameti õigused vastavaid tegevusi nõuda (ESS § 87^2 lg-d 2, 3 ja 5). Ühe lahendusena kitsaskohtade ületamiseks on Majandus- ja Kommunikatsiooniministeerium ja RIA koos partneritega välja töötanud küberturvalisuse seaduse eelnõu, milles sätestatakse riikliku järelevalve meetmed küberturvalisuse valdkonnas, kaasaarvatud RIA õigused ja kohustused riikliku järelevalve teostamisel. Samuti on eelnõuga seotud üks olulisemaid eesmärke NIS direktiivi ülevõtmine.

Küberturvalisuse seaduse eelnõu koostajad on soovinud muuhulgas leida lahenduse seni seaduse tasandil reguleerimata küsimusele, mis puudutab RIA volitusi riikliku ja haldusjärelevalve teostamisel. Kuid mitmed probleemid on endiselt lahendamata. Esiteks on siiani ebaselge RIA täpne roll küberturvalisuse tagamisel. Ka KAPO-l ning Politsei- ja Piirivalveametil on küberturvalisuse tagamiseks ettenähtud ülesanded – KAPO-l vastavalt Eesti Vabariigi vastu suunatud luure- ja õõnestustegevuse vastased (põhimäärus § 8 p 5)[120] ning

[114] Sadamaseadus. – RT I, 03.03.2017, 24.
[115] Raudteeseadus. – RT I, 16.05.2017, 3.
[116] Lennundusseadus. – RT I, 03.03.2017, 16.
[117] Vt Advokaadibüroo LEXTAL. Kübervaldkonna õigusanalüüs, 2016 (viide 118); Advokaadibüroo SORAINEN. Riigi Infosüsteemi Ameti järelevalve meetmed haldusjärelevalvemenetluses ning häda- ja eriolukorras, 2017 (viide 158). Valdkondliku seaduse kehtestamise vajaduse kohta on käesoleva magistritöö autor koostanud uurimistöö. Vt H. Ojamaa. Küberturvalisuse õiguslik reguleerimine ja muudatuste vajadus Eestis. Uurimistöö. Tallinn: TÜ õigusteaduskond 2015. (Käsikiri autori valduses).
[118] Advokaadibüroo LEXTAL. Kübervaldkonna õigusanalüüs, 2016, lk 28. – https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf (21.04.2018).
[119] Küberturvalisuse teenistuse 2015. aasta kokkuvõte, lk 4, 12; Küberturvalisuse teenistuse 2016. aasta kokkuvõte, lk 14-15.
[120] Kaitsepolitseiameti põhimäärus. SiMm 29.10.2014 nr 46. – RT I, 10.10.2017, 11.

Politsei- ja Piirivalveametil võrgu- ja infosüsteemidega seotud süütegude kohtueelse menetlemise (kriminaalmenetluse seadustik § 212 lg 1 ja 4)[121] ülesanded. Lisaks on andmekaitse alane järelevalvepädevus Andmekaitse Inspeksioonil (AvTS § 45 lg 1). KüTS eelnõu § 13 lõikes 1 on sätestatud üldine pädevusnorm, mille kohaselt RIA koordineerib küberturvalisuse tagamist, küberintsidentide ennetamist ja lahendamist eelnõus sätestatud ulatuses, kuid koordineerimise sisu ei muutu sellega selgemaks. Probleemi üks põhjuseid on see, et küberturvalisuse seaduse eelnõus ei ole küberturvalisuse mõistet defineeritud ega sisu avatud, mis annab võimaluse ka valdkondliku järelevalve sisu ja piire erinevalt tõlgendada. Tegemist on seadusandja kaalutluskohaga, milliste meetmete rakendamine on otstarbekas anda RIA pädevusse ja millised meetmed peaksid jääma teiste ametite pädevusse.

Teiseks ei anna küberturvalisuse seaduse eelnõu selget vastust, kas küberintsident on käsitatav korrarikkumisena. Eelnõus kasutatavad mõisted erinevad korrakaitseseaduses kasutatud ohuga seonduvatest mõistetest ja nende omavahelisi seoseid pole otsesõnu selgitatud. Sellest, kas küberintsidenti käsitatakse korrarikkumisena, sõltub ka riikliku järelevalve meetmete rakendamine, kuna see toetub omakorda korrakaitse loogikale. Analüüsi eelnevas osas asuti seisukohale, et küberintsidenti saab käsitada korrarikkumisena. Kuna RIA-le on kavandatud küberturvalisuse seaduse eelnõuga volitusnormid hulga riikliku järelevalve meetmete rakendamiseks, siis eelnõu koostajad on tõenäoliselt seda ka nii ette näinud.

Eelnevates peatükkides kirjeldatud raamistiku põhjal analüüsitakse käesolevas töö osas RIA rakendatavaid riikliku järelevalve meetmeid küberturvalisuse tagamiseks. KüTS eelnõu § 6 punktis 5 on otseselt rõhutatud põhiõiguste kaitse põhimõtet – küberturvalisuse tagamisel kindlustatakse eelnõu kohaselt põhiõiguste ja -vabaduste ning isikuandmete ja identiteedi kaitse. Samuti on kehtivas küberjulgeoleku strateegias tunnustatud proportsionaalsust kui valdkonda üht läbivat põhimõtet.[122] Sellega seoses on analüüsi fookuses nii korrakaitseseaduses sätestatud kui küberturvalisuse seaduse eelnõus planeeritud riikliku järelevalve meetmete rakendamiseks RIA pädevuse olemasolu ning vastavate meetmete kooskõla põhiseadusega. Hinnatud on riivevolituse seisukohast olulist meetme ennetusliku ja ohutõrjelise funktsiooni eristamist, samuti meetme proportsionaalsust ehk sobivust, vajalikkust ja mõõdukust soovitud eesmärgi saavutamiseks. Sarnase sisuga meetmeid on analüüsitud koos või meetme osasid eraldi, kui autor nägi selleks vajadust. Autor rõhutab, et analüüsi abstraktsiooniaste on suur,

[121] Kriminaalmenetluse seadustik. – RT I, 05.12.2017, 8.
[122] Eesti Vabariigi Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014–2017, lk 7. – https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (21.04.2018).

mistõttu pole võimalik ammendava seisukoha andmine kõikideks elulisteks juhtumiteks ja konkreetset olukorda arvestades on meetme kohaldamise igakordne kaalumine vältimatu.

3.1.1. Teavitamine

Korrakaitseorganil on KorS § 26 lõike 1 kohaselt oma pädevuse piires õigus avalikkust või isikut teavitada ohu ennetamisest, ohukahtlusest, ohust või korrarikkumisest. RIA pädevus küberturvalisuse valdkonnas teavitamise meetme rakendamiseks tulenes seni asutuse põhimääruse § 9 punktist 3, mille kohaselt RIA annab hoiatusi turvaintsidentide ennetamiseks, tegeleb kasutajate turvateadlikkuse tõstmisega ning koostab raporteid Eesti arvutivõrkudes toimunud intsidentidest ja pahavara levikust. KüTS eelnõu § 13 lõikes 3 on sätestatud RIA ülesanne riikliku küberturvalisuse tagamise eesmärgil ohuteateid edastada. Kuigi küberturvalisuse seaduse eelnõus ei ole säte paigutatud 4. peatükki, mis reguleerib riikliku ja haldusjärelevalve meetmete rakendamist, on käesoleva töö autori hinnangul normi sisu tõlgendades tegemist riikliku järelevalve erimeetmega. Täpsemalt on eelnõu seletuskirja kohaselt soovitud kehtestada RIA-le volitusnorm nii otseste kui kaudsete küberohtude kohta ohuteadete edastamiseks, eesmärgiga küberintsidendi mõju vältida või vähendada.[123] Norm on aga sõnastatud pädevusnormina, millega RIA-le antakse ülesanne teavitada küberohtudest, mitte volitusnormina, millega sätestatakse organi õigusi ja kohustusi.

Normihierarhiast tulenevalt kuulub eri- ja üldmeetme konkurentsi korral kohaldamisele esmalt erimeede. Erimeetme puudumisel on korrakaitseorganil võimalik kohaldada üldmeedet ka juhul, kui selleks pole ette nähtud vastavat volitusnormi. Seega üldreegli kohaselt oleks RIA-l erimeetme puudumisel võimalik kohaldada üldmeetmena teavitamist KorS § 26 lõike 1 alusel. Teavitamise vormidena on KorS § 26 lõige 1 ette näinud teadaanded, soovitused ja hoiatused. Peale KorS §-s 26 sätestatu ei sisalda kehtiv õigus muid nõudeid korrakaitselise teavitamise sisule ega vormile. Meedet on võimalik rakendada nii ohu ennetamise kui tõrje eesmärgil, olles siiski eelkõige suunatud ohu ennetamisele.

Küberturvalisuse valdkonnas on teavitamine RIA tegevuse eesmärke silmas pidades kahtlemata sobiv meede nii võimalikust küberintsidendist tuleneva ohu realiseerumise vältimiseks kui juba asetleidnud intsidendi mõjude piiramiseks. Korrakaitseseaduse eelnõu seletuskirja kohaselt on teavitamise puhul tegemist korrakaitselise teabetoiminguga, mis on mittesiduva iseloomuga

[123] Küberturvalisuse seaduse eelnõu seletuskiri, lk 22.

ehk isikul puudub selle järgimiskohustus.[124] Ka küberturvalisuse seaduse eelnõus märgitakse, et tegemist võib olla nii konkreetsest küberintsidendist teavitamise kui üldisemat laadi soovituse edastamisega. Teavitamise eesmärk on vähendada riske küberintsidentide toimumiseks, piiramata sealjuures teavitamise viisi ja sihtrühma.[125] Näiteks teavitab RIA intsidentide käsitlemise osakond (CERT Eesti) avastatud turvanõrkustest operatiivselt Twitteri ja blogi vahendusel[126], samuti vajadusel kasutades üleriigilisi meediakanaleid. Siiski ei pruugi praktikas teavitamisega oodatud mõju kaasneda, juhul kui puudutatud isikud ei võta neile antud soovitusi või hoiatusi piisavalt tõsiselt.

Kuna teavitamise puhul on tegemist üksikisikut ja avalikkust ühe vähim koormava ning enamasti väikeste kuludega rakendatava riikliku järelevalve meetmega, siis tõenäoliselt puuduvad vähem koormavad alternatiivsed meetmed. Teavitamisega üldjuhul ei kaasne märkimisväärset põhiõiguste ja -vabaduste riivet, kuid hoolimata meetme mittesiduvast iseloomust, ei saa riive olemasolu siiski välistada. Korrakaitseseaduse kommenteeritud väljaandes on märgitud, et praktikas peetakse teadlikult ja oskuslikult rakendatud teavitamist probleemi lahendamiseks samaaegselt tõhusaimaks ja leebemaiks meetmeks. Siiski on HMS § 107 lg 1 kohaselt nõutav seaduslik alus õiguste ja vabaduste piiramisest teavitamiseks. Õigusi ja vabadusi mitteriivavaks on peetud isikule saadetavat teavitust, mille eesmärgiks on kujundada isiku käitumist läbi informeerimise.[127]

Meetme võimalik riive puudutab PS §-st 19 tulenevat õigust vabale eneseteostusele ja PS §-st 31 tulenevat ettevõtlusvabadust, kuna teavitamise sisu võib olla näiteks üleskutse hoiduda mingisugusest tegevusest interneti vahendusel. Riivega tuleb arvestada ka juhul, kui teavitamisega kaasneb isikuandmete avalikustamine, mis on seotud PS § 26 esimesest lausest tuleneva õigusega eraelu puutumatusele. Kuivõrd KorS § 26 lõige 2 lubab isikuandmete avalikustamist sellisel juhul ja sellises ulatuses, kui see on vältimatult vajalik ohukahtlusest, ohust või korrarikkumisest teavitamiseks, peaks teavitamisel olema põhiõiguste riive viidud miinimumini ning seega meetme rakendamine mõõdupärane. Ka KüTS eelnõu § 13 lõike 3 puhul märgivad koostajad, et avalikkusele edastatakse teavet üldistatud kujul, et isikute eraelu ja ettevõtlusvabadust mitte kahjustada.[128] Riive olemasolul tuleb tuvastada meetme kohaldamise eeldused, hinnata mõju ning võimaldada menetlusosalise ärakuulamise HMS § 40

[124] Korrakaitseseaduse eelnõu seletuskiri, lk 50–51.
[125] Küberturvalisuse seaduse eelnõu seletuskiri, lk 22.
[126] Vt CERT-EE Twitteris https://twitter.com/CERT_EE ja RIA blogi https://blog.ria.ee/ (21.04.2018).
[127] M. Laaring. KorS § 26/2, 3.1., 5.1. – M. Laaring, S. Pars, H. Kranich jt. Korrakaitseseadus: kommenteeritud väljaanne. Tallinn: Sisekaitseakadeemia, 2017.
[128] Küberturvalisuse seaduse eelnõu seletuskiri, lk 22.

lg 2 kohaselt. Juhul kui ohukahtlus ei osutu põhjendatuks, tuleb teavitamisega huvisid kahjustatud isiku nõudmisel või kaaluka huvi korral ka ilma vastava taotluseta anda teada ohu puudumisest.[129] Kokkuvõttes saab teavitamise riikliku järelevalve meetmena küberturvalisuse valdkonnas hinnata nii ohu ennetamise kui ohutõrje aspektist proportsionaalseks, kuna see on oma olemuselt minimaalselt põhiõiguseid ja -vabadusi riivav.

3.1.2. Ettekirjutus

KorS § 28 lõige 1 näeb riikliku järelevalve üldmeetmena ette ettekirjutuse tegemise võimaluse: ohu või korrarikkumise korral on pädeval korrakaitseorganil õigus ettekirjutusega panna avaliku korra eest vastutavale isikule ohu tõrjumise või korrarikkumise kõrvaldamise kohustus. Samuti on korrakaitseorganil õigus hoiatada avaliku korra eest vastutavat isikut KorS § 28 lõigetes 2 ja 3 nimetatud haldussunnivahendite kohaldamise eest, kui isik ei täida kohustust hoiatuses määratud tähtaja jooksul. Pädevus anda õigusaktidega ettenähtud juhtudel ettekirjutusi on RIA põhimääruse § 15 punkti 14 kohaselt RIA peadirektoril. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1, mille kohaselt RIA koordineerib küberintsidentide ennetamist ja lahendamist.

Ettekirjutuse tegemise eesmärk on KorS § 28 lõike 1 kohaselt ohutõrjeline – olenevalt olukorrast ohu tõrjumine või kõrvaldamine korrakaitseorgani määratud tähtaja jooksul.[130] Küberturvalisuse valdkonnas omab ettekirjutuse kohaldamine ohutõrje eesmärgil tõenäoliselt piiratud mõju. Küberintsidendi korral tuleb arvestada, et konkreetse ohuallika tuvastamine võib osutuda keeruliseks, samas on intsidendi mõju piiramine või kõrvaldamine ajakriitiline. Seega võib osutuda ettekirjutus sobivaks ja vajalikuks meetmeks juba ohtu ennetavas perspektiivis. Erimeetme kohaldamine ohu ennetamiseks on KorS § 24 lõike 1 kohaselt lubatud, kui ohuprognoosile tuginedes on võimalik olukord, mille realiseerumisel tekib oht, kuid selleks peab olema seadusest tulenev alus ja kord (KorS § 24 lg 3).

Ettekirjutuse saab KorS § 28 lõike 1 sõnastuse kohaselt teha vaid KorS § 15 lõike 1 tähenduses avaliku korra eest vastutavale isikule. Isikule ettekirjutuse tegemise põhjus KorS § 28 lõike 1 alusel on reeglina ettenähtud nõuete mittetäitmine. Selleks, et nõuete täitmisele asjakohast hinnangut anda, peavad need olema piisava detailsusega kehtestatud. Sarnaselt teavitamisega võib ettekirjutuse mõju ohutõrje seisukohast osutuda tagasihoidlikuks, sest olukorras, kus

[129] M. Laaring. KorS § 26/6.2.
[130] S. Pars. KorS § 28/3.4.

küberintsidendi tagajärjed on juba saabunud, on võimalik veel täiendavaid kahjusid vältida või vähendada, aga mitte enam ära hoida. Lisaks tuleb arvestada, et meetme rakendamiseks kulub teatud aeg, mida kriitilises situatsioonis napib. Ajakulu toob kaasa juba haldusakti andmiseks toimuv menetlus – ettekirjutus on haldusakt HMS § 51 lõike 1 tähenduses. HMS § 55 lõike 2 kohaselt antakse haldusakt üldreeglina kirjalikus vormis. Muus vormis, näiteks suulise ettekirjutuse, võib anda vaid edasilükkamatu korralduse.

Hoolimata eelkirjeldatud riskidest saab ka ettekirjutuse hinnata üldjoontes ohutõrje eesmärgi saavutamisel vajalikuks. KorS § 28 lõike 1 alusel saab avaliku korra eest vastutavat isikut kohustada küberintsidendist tulenevat ohtu tõrjuma või korrarikkumist kõrvaldama. Riigikohus on leidnud, et korrakaitseorgan peab teavituse või ettekirjutuse puhul olema veendunud, et sellest piisab avaliku korra tagamiseks ehk avaliku korra eest vastutav isik tõrjub ohu viivitamatult.[131] Ettekirjutus võib vastavalt olukorrale osutuda sobivaks, et küberintsidendi levik peatada ning taastada rünnaku alla sattunud süsteemis tavapärane olukord. Näiteks oleks ettekirjutuse tegemine asjakohane, kui sideteenuse operaatori vea tõttu ei saa inimesed hädaabinumbril 112 helistada. Taoline probleem ilmnes 24. jaanuaril 2018 Elisa võrgus.[132] Selguse huvides võiks lisaks eelnimetatud üldmeetmele kaaluda küberturvalisuse valdkonna eripära arvestava erimeetme kehtestamist.

Ettekirjutusega kaasneb adressaadi põhiõiguste riive. Meetme rakendamisel toimuva teenuse osutaja tegevuse piiramisel on asjakohane käsitleda eelkõige ettevõtlusvabaduse riivet. Siiski annab PS § 31 teine lause võimaluse paragrahvi esimesest lausest tulenevat vabadusõigust seaduses sätestatud alustel või korras piirata. Ettevõtlusvabaduse sisu seisneb eelkõige selles, et riik ei tohiks ettevõtlust põhjendamatult takistada. Riigikohus on leidnud, et igasugune tegevus, mis takistab, kahjustab või kõrvaldab mõne ettevõtlusega seotud tegevuse, tuleb lugeda ettevõtlust riivavaks.[133] Ettekirjutusega loob aga korrakaitseorgan selle adressaadile õigusliku takistuse ettevõtlusvabadust realiseerida – antud näitel võib ettekirjutuse sisu olla selline, mille kohaselt teenuse osutaja peab piirama teenuse osutamist või astuma muid samme küberintsidendist tuleneva ohu või korrarikkumise kõrvaldamiseks. Samuti on Riigikohus leidnud, et ettevõtlusvabadus on lihtsa seadusreservatsiooniga põhiõigus ja sellele on võimalik seada piiranguid. Sealjuures piisab piirangute kehtestamiseks igast mõistlikust põhjusest.[134]

[131] RKKKo 3-1-1-84-16, p 48.
[132] Vt näiteks https://geenius.ee/uudis/elisa-vea-tottu-ei-saanud-paev-otsa-112-helistada-firma-jattis-sellest-teavitamata/ .
[133] RKPJKo 3-4-1-6-00, p 11.
[134] RKHKo 3-3-1-75-15, p 19.

Seega sarnaselt muude põhiõiguste riivetega tuleb ka ettevõtluspõhiõiguse riivamisel arvestada sellega, et mida intensiivsem on riive, seda mõjuvam peab olema ka riive põhjus.

Ettekirjutusega võib kaasneda omandipõhiõiguse riive näiteks juhul, kui teenuse osutajat kohustatakse kahjurvara võrgu- ja infosüsteemist eemaldama ega lubata süsteemi kasutamist enne esialgse olukorra taastamist. PS § 32 lõikest 1 tuleneva omandipõhiõiguse kohaselt on igal õiguse kandjal vabadus nii omandi kui sellega sarnaste varaliste õiguste kasutamisel ning ühtlasi ka omal vastutusel ise õiguse kasutamist kujundada.[135] Samuti on lõikest 2 tulenevalt omanikul õigus oma omandit vabalt vallata, kasutada ja käsutada, kuid mitte üldiste huvide vastaselt. Riigikohus on asunud seisukohale, et PS § 32 kaitse alla kuuluvad varalised õigused, mh asjad, raha ja varaliselt hinnatavad õigused ja nõuded.[136] Tõenäoliselt riivab ettekirjutuse tegemine rohkem siiski ettevõtlusvabadust, kuna ettekirjutuse tegemine võib takistada pigem teenuse osutamist, kui omandiõiguse teostamist.

Kehtivas õiguses on põhiõiguseid riivavate piirangute kehtestamiseks teatud võimalused olemas. ESS § 66 lõikes 1 on sätestatud alused, mille kohaselt sideettevõtjad saavad teise lepingupoole suhtes piirata juurdepääsu sidevõrgule – näiteks punkti 5 alusel on piirang õiguspärane, kui tekib oht sidevõrgu terviklikule toimimisele. Olukorras, kus küberintsidendi asetleidmisel teeb korrakaitseorgan ettekirjutuse, võib see olenevalt olukorrast olla nii teenuse osutaja enda või teiste isikute huvide kaitseks kui ka üldisemalt avaliku korra kaitseks suunatud, näiteks kui intsident kujutab endast ohtu elutähtsa teenuse toimimisele. HOS § 33 lõigete 1 ja 2 alusel on eriolukorra juhil õigus eriolukorra väljakuulutamise põhjustanud hädaolukorra lahendamiseks kohustada elutähtsa teenuse osutajat vastava teenuse osutamiseks ja ka kohustada piirama lõppkasutajate võimalust teenust või sidevõrku kasutada, rakendades selleks ettekirjutust ja HOS § 33 lõike 3 alusel vajadusel haldussundi.

Eelnimetatud olukorrad on piisava kaaluga, et meetme rakendamist võiks lugeda proportsionaalseks soovitud eesmärgiga. Täiendavalt võib riikliku järelevalve teostamisel osutuda oluliseks korrakaitseorgani poolt ettekirjutuse tegemise võimalus, et vajadusel saaks pädev korrakaitseorgan teenuse osutajat piirangu seadmiseks kohustada ka n-ö tavaolukorras, mitte vaid hädaolukorras. Näiteks võib vastav vajadus tekkida eelnõu § 7 lõikes 1 sätestatud süsteemi turvameetmete rakendamiseks, eesmärgiga küberintsidente ennetada, kui teenuse osutaja vastavaid nõudeid ei täida. Kokkuvõttes saab lugeda ettekirjutuse tegemise

[135] M. Ernits, A. Kelli, P. Roosma. PõhiS § 32/1.
[136] RKÜKo 3-4-1-1-14, p 88.

küberturvalisuse tagamisel ohutõrje seisukohast proportsionaalseks riikliku järelevalve meetmeks. Kaalumist vääriks küberturvalisuse valdkonnas täiendava erimeetme sätestamine ettekirjutuse tegemiseks ohtu ennetaval eesmärgil väljaspool hädaolukorda.

3.1.3. Haldussunnivahendi kohaldamine ja vahetu sund

Koos ettekirjutuse tegemise võimalusega on korrakaitseseaduses sätestatud tagamismeetmetena haldussunnivahendi kohaldamine ja vahetu sund – kui KorS § 28 lõikes 1 sätestatud ettekirjutust ei täideta, on lõike 2 alusel võimalik kohaldada vastutava isiku suhtes asendustäitmise ja sunniraha seaduses[137] (edaspidi ATSS) ettenähtud vahendeid ja lõike 3 kohaselt omakorda nende mõju puudumisel ka vahetut sundi. Erinevalt ettekirjutusest, sunnirahast ja vahetust sunnist võib asendustäitmist läbi viima kohustada peale avaliku korra eest vastutava isiku ka muu isiku, kuid siiski vaid KorS §-s 16 sätestatud tingimustel. KorS § 28 lõike 4 kohaselt ja sättes nimetatud tingimustel võib ohu tõrjuda ja korrarikkumise kõrvaldada ka ettekirjutust andmata, hoiatust ja täitekorraldust tegemata.

Kuna küberturvalisuse seaduse eelnõu ei näe küberturvalisuse tagamisel riikliku järelevalve erimeetmena ette ettekirjutuse täitmata jätmisel sunnivahendite kohaldamist, on asjakohane analüüsida vastava üldmeetme kohaldamist RIA poolt. Sunnivahendite kohaldamine on lubatud, kui ettekirjutuse tegemisega ei ole soovitud tulemust saavutatud ning isik ei täida kohustust määratud tähtaja jooksul. RIA põhimääruse § 9 punkti 1 kohaselt on ameti põhiülesanne riikliku järelevalve teostamine ameti tegevusvaldkondi reguleerivate õigusaktidega kehtestatud nõuete täitmise üle ja nende nõuete rikkumise korral riikliku sunni rakendamine. Ühtlasi on haldussunnivahendi kohaldamise pädevus seotud ettekirjutuse tegemise pädevusega KorS § 28 lõike 1 kohaselt. Lisaks on üldine pädevusnorm sõnastatud küberturvalisuse seaduse eelnõu § 13 lõikes 1. Olemuselt on analüüsitavad sunnivahendid ohutõrjelised.

Kahtlemata on haldussunnivahendite kasutamine RIA poolt küberturvalisuse tagamisel samavõrd sobiv meede kui ettekirjutuse tegemine. Sunnivahendid on ettekirjutusega tihedalt seotud, aidates saavutada taotletud eesmärki. Sunnimeede peab olema tõhus, otstarbekas ja proportsionaalne ning tagama kohustuse täitmise.[138] Tagamismeetmete kohaldamise kohasuse tingib see, kui ettekirjutus üksinda ei osutu piisavaks ehk olukorras, kus isik keeldub RIA-ga

[137] Asendustäitmise ja sunniraha seadus. – RT I, 12.07.2014, 29.
[138] S. Pars. KorS § 28/4.

koostööst – näiteks ei ole teenuse osutaja täitnud talle tehtud ettekirjutust. Samuti võib meede osutuda asjakohaseks kiirelt leviva ülemaailmse küberrünnaku tõkestamiseks. Iseküsimus on aga vahetu sunni kohaldamise sobivus ja vajalikkus küberturvalisuse valdkonnas RIA kui erikorrakaitseorgani poolt. KorS § 74 lõike 1 kohaselt on vahetu sund füüsilise isiku, looma või asja mõjutamine füüsilise jõuga, erivahendiga või relvaga. Sealjuures on vahetu sunni kohaldamise pädevus politseil ning seaduses sätestatud juhtudel ka muul korrakaitseorganil (KorS § 75 lg 1). Meetme rakendamine peab olema läbimõeldud ja konkreetsele korrakaitseorganile jõukohane. RIA kui erikorrakaitseorgani puhul võiks kõne alla tulla füüsilise jõu või erivahendi kohaldamine, relva kasutamise õigus kujuneks asutuse tegevuse eesmärke silmas pidades ilmselgelt üleliigseks. Näiteks võib küberintsidendi lahendamiseks osutuda vajalikuks hoonesse sisenemisel kasutada füüsilist jõudu. Samas eeldab ka subjekti füüsilise jõu või erivahendiga mõjutamine meedet otseselt kohaldavatelt teenistujatelt teatavat ettevalmistust, oskuseid aga ka valmidust end võimalikes ohuolukordades kaitsta. Otstarbekam on RIA-l kaasata vahetu sunni rakendamise vajadusel politseid tema pädevuse piires ja taotleda HKTS § 18 lõike 1 punkti 1 alusel selleks politsei ametiabi. Vastav kohustus ametiabi osutada tuleb politseile KorS § 6 lõikest 6. Ühtlasi peab olema vahetu sunni kohaldamine lubatav (KorS § 76). Küberturvalisuse tagamise eesmärgil vahetu sunni kohaldamiseks pole küberturvalisuse seaduse eelnõus kavandatud politseile pädevust. Olukorras, kus vahetu sunni kohaldamine on küberintsidendi lahendamiseks vajalik, kuid RIA pole selleks pädev ja ohu tõrjumine pole ühegi korrakaitseorgani pädevuses, võib tekkida vajadus, et politsei osaleb probleemi lahendamisel kui üldkorrakaitseorgan KorS § 6 lõike 2 alusel.

Haldussunnivahendi kohaldamise mõõdukuse analüüsimisel on asjakohased samad aspektid ja argumendid, mis ettekirjutuse puhul. Kuivõrd haldussunnivahendi kohaldamine tuleb kõne alla olukorras, kus ettekirjutusega ei ole saavutatud soovitud eesmärki, siis on õigustatud mõnevõrra suurem subjekti põhiõiguste riive, et soovitud olukorrani jõuda. Põhjalikumat analüüsi ei ole asjakohane siinkohal läbi viia, kuna konkreetse sunnivahendi valik ja ulatus oleneb olukorrast ning vastav kohaldamine peab toimuma ATSS-is sätestatud vahendite ja korraga kooskõlas. Lisaks annab KorS § 28 lõige 2 võimaluse sätestada sunniraha igakordse kohaldamise ülemmäär riikliku järelevalve eriseaduses. Juhul kui seadusandja ei soovi küberturvalisuse seaduse eelnõus teha küberturvalisuse valdkonna puhul erisusi, siis kohaldub ATSS-is ettenähtud sunniraha ülemmäär 9600 eurot. Teatud juhtudel võib vahetu sunni kohaldamine RIA poolt siiski osutuda vajalikuks ning konkreetses situatsioonis tuleks hinnata meetme kohaldamise proportsionaalsust. Kokkuvõttes saab haldussunnivahendi kohaldamist RIA poolt

pidada proportsionaalseks ning meedet seega põhiseadusega kooskõlas olevaks. Hinnang vahetu sunni kohaldamise proportsionaalsusele sõltub käsitletud asjaoludest.

3.1.4. Ohu tõrjumine või korrarikkumise kõrvaldamine korrakaitseorgani poolt ja küberintsidendi tõkestamine

RIA kui küberturvalisuse valdkonnas pädev korrakaitseorgan saab ohu tõrjumiseks rakendada KorS § 29 lõikes 1 sätestatud riikliku järelevalve üldmeedet. Sätte kohaselt võib korrakaitseorgan ise kohaldada meetmeid ohu tõrjumiseks või korrarikkumise kõrvaldamiseks, kui avaliku korra eest vastutavat isikut ei ole, isik kas ei saa või ei saa õigel ajal ohtu tõrjuda või korrarikkumist kõrvaldada. Selleks võib vajaduse korral kasutada ametiabi või kaasata muid isikuid KorS §-s 16 sätestatud tingimustel. Küberturvalisuse seaduse eelnõu sätestab erimeetmena küberintsidendi tõkestamise, millel on üldmeetme ees rakendamisprioriteet. KüTS eelnõu § 17 lõike 1 kohaselt võib RIA riikliku järelevalve teostamisel süsteemi juhtimise vahetult või kaughalduse teel üle võtta ning selle kasutamist või juurdepääsu piirata kõrgendatud ohu väljaselgitamiseks või tõrjumiseks sätte lõikes 2 nimetatud kumulatiivsetel tingimustel. Kuigi küberturvalisuse seaduse eelnõu sellele otsesõnu ei viita, on küberintsidendi tõkestamine sisult sarnane korrakaitseorgani poolt ohu tõrjumise ja korrarikkumise kõrvaldamisega, mistõttu on meetmeid analüüsitud koos.

Pädevus ohu tõrjumiseks ja korrarikkumise kõrvaldamiseks tuleneb RIA põhimääruse § 8 punktist 1 koosmõjus § 9 punktiga 3, mille kohaselt RIA käsitleb Eesti arvutivõrkudes toimuvaid ja ametile raporteeritud turvaintsidente. Sama paragrahvi punkti 1 kohaselt on RIA pädevuses ka kriitilise informatsiooni infrastruktuuri kaitse korraldamine. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Nimetatud üld- ja erimeede on kasutatavad ohutõrjeks.

Küberturvalisuse tagamise seisukohast on küberintsidendi tõkestamine sobiv, kuna intsidendi leviku peatamiseks võib ohu avastamise järgselt olla vajalik riigi sekkumine. Teatud juhtudel võib RIA operatiivne sekkumine osutuda isegi vältimatuks. Sellised olukorrad on nimetatud KüTS eelnõu § 17 lõikes 2, mis on ka ühtlasi kumulatiivselt meetme rakendamise tingimusteks: küberintsident ohustab teise süsteemi turvalisust või avalikku korda, süsteemi haldaja ei saa õigel ajal küberintsidenti lahendada, küberintsidenti ei saa tõkestada või ohtu tõrjuda muu, vähem riivava meetmega ning küberintsidendi tõkestamisega ei või tekitata ebaproportsionaalselt suurt kahju. Meetme kohaldamisel tuleb sellest kiiresti teavitada süsteemi

haldajat ning RIA on kohustatud meetme rakendamist protokollima (KüTS eelnõu § 17 lg-d 3 ja 4). Seega osutub avaliku võimu sekkumine otstarbekaks, kui konkreetsel juhul nähtub vajadus korrakaitseorgani tegevuseks ja tegevus ei kujuta endast ülemäärast õiguste riivet. Meede on asjakohane näiteks küberspionaaži tõkestamisel. Üks taoline intsident leidis RIA andmetel aset 2016. aastal Viru Keemia Grupi arvutivõrgus.[139]

Küberturvalisuse tagamisel peab olema RIA-l võimalus küberintsidendile operatiivselt reageerida, kui olukord tingib vastava vajaduse. Kuna sellise tegevusega võib alati kaasneda kahju tekkimine, siis tuleb igakordselt piisava põhjalikkusega hinnata, kas võimalik kasu kaalub üles kahju tekkimise ja selle ulatuse. Et sekkumist saaks pidada proportsionaalseks, peab rakendatav abinõu olema nii isiku, kelle suhtes seda kohaldatakse, kui ka kolmandate isikute õiguseid võimalikult vähe riivav. RIA tegevuse vajadus küberintsidendi tõkestamiseks tuleneb eelkõige sellest, et võrgu- ja infosüsteemi haldaja ei tule sellega oodatud moel toime, näiteks viivitab intsidendi tõkestamiseks vajalike meetmete kasutuselevõtuga. Seega üldjuhul peaks küberintsidendile asjakohane ja õigeaegne reageerimine olema nii võrgu- ja infosüsteemi haldaja kui ka kolmandate isikute huvides ja sellisel juhul ka vajalik.

Mõõdukuse seisukohast on korrakaitseorgani tegevuste hindamisel olulised põhiõigustesse sekkumise ulatus ja intensiivsus. Sarnaselt ettekirjutusele riivab küberintsidendi tõkestamine tõenäoliselt PS §-st 31 tulenevat õigust ettevõtlusvabadusele, olenevalt olukorrast ka PS § 32 lõike 1 esimeses lauses sätestatud omandiõiguse puutumatust. Samas võib sellisel juhul lugeda riivet põhjendatuks, kui isik ei saa või ei saa õigel ajal talle kuuluvat ohutõrje ülesannet täita või ohtu satuvad kolmandate isikute või laiemalt avalik huvi. Kuna meetmega kaasnev põhiõiguste ja -vabaduste riive võib osutuda intensiivseks, siis on asjakohane sõnastada KüTS eelnõu § 17 lõige 1 detailsemalt. Küberturvalisuse seaduse eelnõu seletuskirjas on märgitud, et tegemist on *ultima ratio* abinõuga.[140] Seda on oluline praktikas järgida ning meedet rakendada vaid juhul, kui muud meetmed on ammendunud. Olukorras, kus küberintsidendi mõju leviku peatamise vajadus kõrgema eesmärgina kaalub üle nimetatud põhiõiguste võimaliku riive, saab selle hinnata mõõdupärasuse tingimusega kooskõlaliseks.

Nii analüüsitud riikliku järelevalve üldmeedet kui ka erimeetmena küberintsidendi tõkestamist küberturvalisuse tagamiseks saab RIA poolt pidada kirjeldatud tingimustel proportsionaalseks. Küberintsidendi tõkestamisega seotud tingimused tuleks siiski eelnõus reguleerida detailsemalt.

[139] Vt Küberturvalisuse teenistuse 2016. aasta kokkuvõte, lk 23.
[140] Küberturvalisuse seaduse eelnõu seletuskiri, lk 25.

Eraldi küsimus on, kas KüTS eelnõu § 17 lõikes 1 sätestatud erimeede on kattuv KorS § 29 lõikes 1 sätestatud üldmeetmega. Juhul kui kavandatav erimeede ei kanna endas küberturvalisuse valdkonna spetsiifikast tulenevat erisust, on ettepanek see antud kontekstis eelnõust välja jätta, sest sisuliselt oleks tegemist üldmeetme kordamisega.

3.1.5. Küsitlemine

Küsitlemine on riikliku järelevalve erimeetmena sätestatud KorS § 30 lõikes 1. Peale politsei on muul korrakaitseorganil õigus isik peatada ja teda küsitleda seaduses sätestatud juhul. Selleks peab pädeval korrakaitseorganil olema konkreetne alus arvata, et isikul on vajalikke andmeid ohu ennetamiseks, väljaselgitamiseks, tõrjumiseks, korrarikkumise kõrvaldamiseks, kaitstava isiku või valvatava objekti ohutuse tagamiseks. RIA kui muu korrakaitseorgani volituse alus meetme rakendamiseks on sätestatud KüTS eelnõu § 16 lõikes 1. RIA pädevus on tuletatav eelkõige asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjakohaste punktidega. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Meede on kasutatav nii ohu ennetamise kui ohu tõrjumise eesmärgil.

Korrakaitseseaduse eelnõu seletuskirjast nähtub, et küsitlemise kui erimeetme rakendamise õigus on antud kõigile korrakaitseorganitele, kui selleks on seaduses sätestatud alus. Samas tuleb arvestada, et küsitlemiseks isiku peatamine on lubatud vaid ajal, mil tema suhtes rakendatakse meedet. See ei tohi muutuda isiku kinnipidamiseks, millel on juba teistsugune eesmärk. Seaduse koostajate hinnangul on küsitlemise puhul tegemist isiku põhiõigusi ja -vabadusi ühe vähim riivava riikliku järelevalve meetmega.[141]

Küberturvalisuse tagamisel on küsitlemine riikliku järelevalve meetmena sobiv ja vajalik RIA-le info hankimiseks ja hindamiseks, kas eksisteerib küberturvalisust ähvardav oht. Näiteks võib selline vajadus tekkida pahavara ohvriks langenud isiku poolt rakendatud turvameetmete kohta esialgse ülevaate saamiseks. Kuivõrd küsitlemise läbiviimine on võimalik erinevatel viisidel, siis on oluline hinnata, kas seda on võimalik teha digitaalseid jm võimalusi kasutades – sh kas isikut võib küsitleda näiteks telefoni teel või digitaalselt serverite omavahelise suhtluse kaudu. Korrakaitseseadus ei anna selget vastust, millisel viisil peab küsitlemise läbi viima ega piira ka kommunikatsioonivahendite kasutamist. Kui isikusamasuse tuvastamine pole konkreetses olukorras määrava tähtsusega, siis puudub üldjuhul ka vajadus küsitlemise vormi

[141] Korrakaitseseaduse eelnõu seletuskiri, lk 54.

piirata, kui see oma eesmärki täidab. Küll aga vajadusel protokollitakse küsitlemise tulemused, kui küsitletav taotleb või peab korrakaitseorgan protokollimist vajalikuks (KorS § 30 lg 2).

Autor ei tuvastanud antud meetme puhul ühegi konkreetse põhiõiguse või -vabaduse märkimisväärset riivet. Korrakaitseseaduse kommenteeritud väljaandes on märgitud, et tegemist on isiku õigusi ja vabadusi ühe vähim riivava ja riiklik järelevalve teostamisel väga vajaliku meetmega. Andmete saamiseks on lubatud pädeval korrakaitseorganil isikut küsitleda, kui isikul on tõenäoliselt ohuga seonduvalt vajalikku teavet.[142] Kõige tõenäolisemalt võib riive puudutada PS §-st 19 tulenevat üldist vabaduspõhiõigust, mis hõlmab endas õigust teha või mitte teha mida iganes, kuivõrd küsitlemine võib piirata teatud ajal selle subjekti liikumist või võimalust viibida soovitud kohas.[143] Samuti võib riive puudutada PS § 26 esimesest lausest tulenevat õigust eraelu puutumatusele. Antud meetme puhul puudub põhjus kahelda selle mõõdukuses, kuna küsitlemise eesmärk on eelkõige saada võimaliku küberturvalisuse ohu kohta informatsiooni, mis ei piira oluliselt küsitletava isiku tegevust. Kokkuvõttes saab hinnata küsitlemise küberturvalisuse tagamisel proportsionaalseks meetmeks RIA-le vajaliku informatsiooni hankimisel nii küberintsidendist tuleneva ohu ennetamiseks kui tõrjumiseks.

3.1.6. Dokumentide nõudmine

KorS § 30 lõike 3 kohaselt on politseil ja muul korrakaitseorganil seaduses sätestatud juhul õigus nõuda riikliku järelevalve erimeetmena isikult dokumentide esitamist. Selleks peab pädeval korrakaitseorganil olema konkreetne alus arvata, et isikul on vajalikke andmeid ohu ennetamiseks, väljaselgitamiseks, tõrjumiseks, korrarikkumise kõrvaldamiseks, kaitstava isiku või valvatava objekti ohutuse tagamiseks. Dokumentide nõudmine tuleb protokollida või muul viisil fikseerida (KorS § 30 lg 4). RIA kui muu korrakaitseorgani volitus dokumentide nõudmiseks on sätestatud KüTS eelnõu § 16 lõikes 1. Sarnaselt küsitlemisele, on RIA pädevus tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjakohaste punktidega – asutuse ülesannete täitmise käigus võib RIA-l tekkida vajadus nõuda isikult dokumente. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Meede on rakendatav nii ohu ennetamise kui ohu tõrjumise eesmärgil.

Kuna RIA-l tõenäoliselt ei ole võimalik küberintsidendist ohustatud või puudutatud võrgu- ja infosüsteemi kohta informatsiooni mujalt hankida kui selle haldajalt, siis võib osutuda

[142] S. Pars. KorS § 30/1, 3.
[143] M. Ernits. PõhiS § 19/3.

asjakohaseks vastavat materjali isikult nõuda. Sarnaselt küsitlemisele saab dokumentide nõudmist riikliku järelevalve meetmena pidada sobivaks ja vajalikuks nii küberintsidendi ennetamise kui intsidendist tuleneva ohu tõrjumise eesmärgil näiteks olukorras, kus on vaja saada informatsiooni võrguliikluse kohta. Näiteks võib olla asjakohane isikult nõuda võrgulogi, et teha kindlaks, kuidas pahavara võrgusüsteemi sattus. Problemaatiliseks võib osutuda selliste teabeallikate väljanõudmine KorS § 30 lõike 3 alusel, mis ei ole üheselt dokumendina käsitatavad.

Dokument on defineeritud arhiiviseaduse[144] § 2 lõikes 1: dokument on mis tahes teabekandjale jäädvustatud teave, mis on loodud või saadud asutuse või isiku tegevuse käigus ning mille sisu, vorm ja struktuur on küllaldane faktide või tegevuse tõendamiseks. Küberturvalisuse seaduse eelnõu seletuskiri ei anna vastust, kas näiteks võrgu- ja infosüsteemis toimuva andmeliikumise logi (võrgulogi) või infosüsteemi logi on käsitatav dokumendina. Kogutud andmete põhjal informatsiooni saamiseks ja järelduste tegemiseks on need vaja esmalt läbi töötada, mistõttu üks võimalik seisukoht on, et jooksvalt kogutav ja salvestatav teave ei kvalifitseeru dokumendiks. Samas võimaldab eelnevalt viidatud arhiiviseaduse säte tõlgendust, et andmete liikumise protokoll või infosüsteemi logi on siiski käsitatav dokumendina, kuna tegemist on jäädvustatud teabega, mis on saadud kellegi tegevuse käigus ja nende andmete abil on võimalik tegevust tõendada. Vaidluse korral kujuneb mõiste lõplik sisustamine kohtupraktikas, kuid õigusselguse tagamiseks oleks võimalik lahendus küberturvalisuse seaduse eelnõus RIA-le antavat volitusnormi täpsustada ning sätestada konkreetsemalt, mille suhtes on RIA-l nõudeõigus või defineerida dokumendi mõiste küberturvalisuse seaduse tähenduses.

Dokumentide nõudmisel võib RIA tegevus riivata isiku õigust ettevõtlusvabadusele, mis tuleneb PS § 31 esimesest lausest. Näiteks võib dokumentides sisalduda teavet, mis on liigitatav ärisaladuse alla ning mille sattumine kolmandate osapoolte kätte võib kahjustada ettevõtja huve. Siiski on riikliku järelevalve korras korrakaitseorgani huvi küberintsidente ennetada või selgitada ohutõrje eesmärgil välja küberintsidendiga seonduvad asjaolud, sh hinnata selle mõju, peatada levik, taastada algne olukord vms, mis kaalub üles ettevõtlusvabaduse riive. Samuti kaitstakse seeläbi kolmandate isikute ja riigi huve laiemalt, eesmärgiga piirata intsidendi mõju levikut. Kokkuvõttes saab ka dokumentide nõudmist pidada proportsionaalseks riikliku järelevalve meetmeks, mille rakendamine küberturvalisuse tagamise eesmärgil on põhiseadusega kooskõlas.

[144] Arhiiviseadus. – RT I, 06.01.2016, 6.

3.1.7. Kutse ja sundtoomine

Politseil ja seaduses sätestatud juhul on muul korrakaitseorganil KorS § 31 lõike 1 alusel riikliku järelevalve erimeetmena õigus kutsuda isik ametiruumi. Selleks peab pädeval korrakaitseorganil olema konkreetne alus arvata, et isikul on vajalikke andmeid ohu ennetamiseks, väljaselgitamiseks, tõrjumiseks, korrarikkumise kõrvaldamiseks, kaitstava isiku või valvatava objekti ohutuse tagamiseks. RIA kui muu korrakaitseorgani volitus kutse kohaldamiseks on sätestatud KüTS eelnõu § 16 lõikes 1. RIA pädevus on tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjakohaste punktidega – asutuse ülesannete täitmise käigus võib RIA-l tekkida vajadus isik kutsuda ka ametiruumi. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Kutse on rakendatav nii ohu ennetamise kui ohu tõrjumise eesmärgil.

KorS § 31 lõike 4 kohaselt võib isiku suhtes kohaldada sundtoomist, kui on alust arvata, et isikul on olulist teavet, mis on vajalik kõrgendatud ohu tõrjumiseks ning lõike 2 kohaselt on isikut sundtoomise eest eelnevalt hoiatatud. Seega on tegemist kitsamalt ohutõrje eesmärgil rakendatava meetmega – kui on ilmnenud kõrgendatud oht KorS § 5 lõike 4 tähenduses. RIA pädevus ja volitus piirdub korrakaitseõigusest tulenevate võimaluste kohaselt kutse kohaldamisega ja mitteilmumisel sunniraha määramisega KorS § 31 lõike 3 alusel. Sundtoomist saab KorS § 31 lõike 5 kohaselt rakendada vaid politsei, kui kutse on andnud muu selleks pädev korrakaitseorgan. Kuna RIA-l puudub isiku ametiruumi sundtoomiseks pädevus, siis oleks asjakohane taotleda HKTS § 18 lõike 1 punkti 1 alusel selleks politsei ametiabi. Vastav kohustus tuleb politseile KorS § 6 lõikest 6, kuid toiminguks peab olema samuti selge pädevus. Sarnaselt vahetu sunni kohaldamisega võib tekkida vajadus, et politsei osaleb olukorra lahendamisel kui üldkorrakaitseorgan KorS § 6 lõike 2 alusel, kuna pädevust küberturvalisuse seaduse eelnõust kui eriseadusest politseile küberturvalisuse tagamise eesmärgil sundtoomise kohaldamiseks ei tulene.[145]

Kutset puudutav üldregulatsioon on sätestatud HMS §-s 17, mis hõlmab ka kutses sisalduvat kohustuslikku teavet. Täiendavalt tuleb KorS § 31 lõike 2 kohaselt arvestada ka korrakaitsest tulenevaid erisusi. Üks selliseid erisusi on hoiatuse tegemise kohustus: kui on alust arvata, et isikul on olulist teavet, mis on vajalik kõrgendatud ohu tõrjumiseks, siis peab kutse KorS § 31

[145] Vt ka KorS § 31 kommentaarid (viide 127).

lõike 2 teise lause järgi sisaldama hoiatust, et isiku ilmumata jäämise korral võib tema suhtes kohaldada sundtoomist.

Kutse ja eelkõige selle eiramisel isiku sundtoomine ametiruumi on oma olemuselt selgelt isiku põhiõiguseid ja -vabadusi riivavad. Küsitav on see, kas küberturvalisuse tagamise eesmärgil peaks kutset isiku suhtes kohaldama esimese valikuna. Sobivaks ja vajalikuks võiks osutuda antud meetme rakendamine eelkõige olukorras, kus näiteks küsitlemine ja dokumentide küsimine ei ole andnud tulemusi ning isikuga on vajalik otsesem suhtlus. Ohu ennetamise eesmärgil kutse kohaldamisel tuleb arvestada KorS § 31 lõikes 10 sätestatut, mille kohaselt võib kutsuda isiku ametiruumi, kui küsitlemise või dokumentide nõudmise kohaldamine muul isikut vähemkoormaval viisil ei ole võimalik. Sobivaks ja vajalikuks meetmeks saab sundtoomist pidada eelkõige kõrgendatud ohu korral. Näiteks võib kutse osutuda asjakohaseks, kui esineb vajadus, et isik tooks küberintsidendist puudutatud seadmed RIA-sse kontrollimiseks. Kui tekib vajadus isiku sundtoomiseks ametiruumi, on RIA-l võimalik kasutada politsei ametiabi.

Põhiõigustest riivab kutse kohaldamine PS § 34 esimese lausega kaitstavat õigust vabalt liikuda, kuna isik on toimingu ajal ametiruumis, kus tal tuleb informatsiooni andmiseks viibida. Sundtoomine riivab ka PS § 20 lõike 1 kohaselt õigust isikupuutumatusele. Kinnipidamisega piiratakse isiku vabadust menetlustoimingu ajal ulatuslikumal määral, kui seda tehakse kutse kohaldamisel. Sellisel juhul on isik oma eelneva tegevusetusega andnud suuremaks riiveks ka põhjuse. Siiski on vahetu sunni kohaldamine lubatud nii kaua, kui see on eesmärgi täitmiseks vajalik (KorS § 31 lg 9). Kutset saab lugeda riikliku järelevalve meetmetena küberturvalisuse valdkonna vajadusi arvestades nii sobivaks, vajalikuks kui mõõdukaks, kui isik kutsutakse ametiruumi eesmärgiga saada informatsiooni, et seda kasutada küberintsidendist tuleneva ohu ennetamiseks või tõrjeks näiteks olukorras, kus küsitlemise ja dokumentide nõudmise puhul pole isik küsitud teavet esitanud. Liikumisvabadust ja isikupuutumatust on õigus riivata vaid piiratud aja vältel. Sundtoomise puhul tuleb arvestada ka lisatingimusega, et erinevalt kutsest on see õiguspärane kõrgendatud ohu tõrjumise vajaduse korral ning seda ei ole lubatav rakendada inspektsioonilise järelevalve käigus.

3.1.8. Isikusamasuse tuvastamine

Riikliku järelevalve erimeetmena võib nii politsei kui seaduses sätestatud juhul muu korrakaitseorgan isiku teadmisel kehtiva isikut tõendava dokumendi alusel tuvastada isikusamasuse KorS § 32 lõikes 1 sätestatud viisil, kui see on vajalik ohu ennetamiseks,

väljaselgitamiseks, tõrjumiseks või korrarikkumise kõrvaldamiseks. RIA kui muu korrakaitseorgani volitus isikusamasuse tuvastamise kohaldamiseks on sätestatud KüTS eelnõu § 16 lõikes 1. Sarnaselt mitme käesolevas töös eelnevalt käsitletud meetmega, on RIA pädevus tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjakohaste punktidega – oma ülesannete täitmise käigus võib RIA-l tekkida vajadus teha isik kindlaks. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Isikusamasuse tuvastamine on rakendatav nii ohu ennetamise kui ohu tõrjumise eesmärgil.

Isikusamasuse tuvastamine on korrakaitseseaduse eelnõu seletuskirja järgi sobiv peamiselt avalikku korda ähvardava ohu aga ka ohukahtluse ja korrarikkumise korral. Säte on sõnastatud viisil, et meedet on võimalik rakendada ka ohu ennetamiseks. Meetme sisuks on õigus peatada isik, sh isiku sõidukis viibimise korral sõiduk, nõuda isiku tõendamist identifitseeriva dokumendi alusel ja saada temalt ütlusi isiku tuvastamise eesmärgil.[146] Isikusamasuse tuvastamise eesmärk on üldine – kas kontrollitava isiku ütlused enda isiku kohta on vastavuses tegelikkusega. Ka küberturvalisuse valdkonnas annab meetme rakendamine RIA-le võimaluse isikuandmeid kontrollida. Isikusamasuse tuvastamine on võimalik KorS § 32 lõike 1 kohaselt erinevate tegevuste abil, sh nime ja sünniaja kindlakstegemisega, dokumendiga tutvumisel, foto ja biomeetriliste andmete võrdlemisel isikuga jm õiguspärasel viisil, mis võimaldab isiku kindlakstegemist. Praktikas võib isikusamasuse tuvastamise osutuda asjakohaseks näiteks olukorras, kus isikule tagastatakse RIA poolt kontrollitud küberintsidendiga seotud seadmed.

Esimene küsimus tekib viisi kohta, kuidas RIA saab isikusamasust kontrollida. KorS § 32 lõike 4 kohaselt võib korrakaitseorgan dokumendile kantud või isiku antud andmete õigsust kontrollida rahvastikuregistrist või muust Euroopa Liidu õigusakti või seaduse alusel loodud andmekogust. Riigiasutusele on võimalik anda ligipääs rahvastikuregistri andmetele avalike ülesannete täitmiseks ning selleks sõlmitakse andmete töötlemise leping (rahvastikuregistri seaduse[147] § 70 lg-d 1 ja 3). Seega vajab konkreetsete viiside planeerimisel põhjalikumat läbimõtlemist, millises ulatuses on RIA-l vaja rakendada riikliku järelevalve meetmena isikusamasuse tuvastamist ning millisel viisil seda hakatakse tegema. Teiseks, isikusamasuse tuvastamisel tuleb tagada andmete kaitse. Nii rahvastikuregistrisse kui ka muudesse andmekogudesse isiku kohta päringute tegemine loetakse isikuandmete töötlemiseks isikuandmete kaitse seaduse[148] (edaspidi IKS) § 5 tähenduses ning andmete töötleja on

[146] Korrakaitseseaduse eelnõu seletuskiri, lk 55–56.
[147] Rahvastikuregistri seadus. – RT I, 10.03.2017, 6.
[148] Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10.

kohustatud järgima IKS §-s 6 sätestatud isikuandmete töötlemise põhimõtteid. Lisaks tuleb arvestada, et analüüsitavas korrakaitseseaduse sättes nimetatud biomeetrilised andmed on delikaatsed isikuandmed IKS § 4 lõike 2 punkti 5 tähenduses ning sellistele andmetele kehtivad veelgi rangemad andmekaitsenõuded. Seega tuleb enne meetme rakendama asumist tagada, et RIA täidab andmete töötlemisel seadusest tulenevaid nõudeid.

Hinnates meetme eesmärgi suhtes üldjoontes sobivaks, tekib siiski küsimus selle rakendamise vajalikkuse kohta. Järelevalvekohustusi täites on RIA huvi seoses küberintsidentidega pigem võrgu- ja infosüsteemide kui konkreetsete isikutega seotud. Samas ei saa järelevalvekohustusi täites välistada vajadust kontrollida ka isikusamasust, kui konkreetne menetlustoiming seda nõuab, näiteks küsitlemisel isikusamasuses veendumiseks. Meetmel ei ole RIA jaoks tõenäoliselt järelevalveülesannete täitmisel otsest sisulist väärtust, vaid selle rakendamine on asjakohane koos teiste riikliku järelevalve meetmetega, kui olukord tingib vastava vajaduse. Meetme rakendamine on asjakohane ohutõrje eesmärgil. Kuivõrd ohu ennetamiseks riikliku järelevalve meetme rakendamine peab olema veelgi selgemalt põhjendatud kui ohutõrje puhul, siis on küberturvalisuse valdkonnas isikusamasuse tuvastamise vajadus ohu ennetamiseks küsitav.

Kuivõrd isikusamasuse tuvastamisel on puutumus isikuandmete töötlemisega, siis on asjakohane Eesti Vabariigi põhiseaduse kontekstis analüüsida PS § 19 kaitsealasse jäävat üldise vabaduspõhiõiguse riivet, sest isikusamasuse kindlakstegemine ei kujuta endast mõne teise konkreetsema põhiõiguse riivet. Eraelu on kaitstav õigushüve Euroopa Inimõiguste konventsiooni artikkel 8 kohaselt, kohtupraktikas on vastavasse kaitsealasse arvatud muuhulgas isiku identifitseerimise kaitse.[149] Riigikohus on leidnud, et tegemist on lihtsa seadusreservatsiooniga põhiõigusega, mistõttu õiguse piiramine on võimalik erinevatel põhjustel, mida PS otsesõnu ei välista.[150] Kuna isikusamasuse tuvastamine reeglina ei kujuta endast intensiivset ega ulatuslikku isiku põhiõigustesse sekkumist, siis saab meedet pidada ka küberturvalisuse tagamise eesmärgil mõõdukaks. Kokkuvõttes võib isikusamasuse tuvastamist küberturvalisuse valdkonnas pidada ohutõrje eesmärgil üldjoontes proportsionaalseks riikliku järelevalve meetmeks. Konkreetsema hinnangu andmiseks on vaja selgemat ülevaadet, kuidas RIA kõnealust meedet asub rakendama.

[149] K. Jaanimägi, L. Oja. PõhiS § 26/4.
[150] RKTKo 3-2-1-152-09, p 11.

3.1.9. Isikuandmete töötlemine andmete saamisega sideettevõtjalt ja sideettevõtja kohustus andmeid esitada

Kõrgendatud ohu väljaselgitamiseks või tõrjumiseks on KorS § 35 lõike 1 kohaselt politseil ja seaduses sätestatud juhul muul korrakaitseorganil õigus töödelda isikuandmeid ja teha nende saamiseks kirjalik või elektrooniline päring ESS § 111^1 lõigetes 2 ja 3 ning § 112 lõikes 3 nimetatud mobiiltelefonivõrgus kasutatavate terminalseadmete asukoha tuvastamist reaalajas võimaldavate andmete saamiseks. KorS § 35 lõikes 1 sätestatud riikliku järelevalve meede on suunatud sellise isiku kohta andmete saamisele, kelle puhul see on vajalik kõrgendatud ohu väljaselgitamiseks või tõrjumiseks. KüTS eelnõu § 22 lõige 5 sisaldab rakendussätet ESS-i täiendamiseks §-ga 114^3, mille kohaselt on sideettevõtjal kohustus RIA päringu alusel sättes nimetatud andmeid esitada, mis võimaldavad küberintsidendi põhjustatud seadme või küberintsidendist ohustatud seadme välja selgitada. Seega sätestatakse RIA-le volitusnorm vastavaid andmeid nõuda. RIA pädevus sideandmete saamiseks on tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjakohaste punktidega. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1.

Kui KorS § 35 lõige 1 on selgelt ohutõrje eesmärgil kasutatav meede (kõrgendatud ohu väljaselgitamiseks või tõrjumiseks), siis KüTS eelnõu § 22 lõike 5 sõnastusest eesmärk üheselt välja ei tule. Küberintsidendi põhjustanud seadme väljaselgitamine on küll ohu tõrjumise alla liigitatav, kuid küberintsidendist ohustatud seadme väljaselgitamise eesmärk võib teoreetiliselt olla nii ohu ennetamine kui tõrjumine. Eelkõige on meede asjakohane olukorras, kus on vaja välja selgitada pahavara leviku algallikas. Õigusselguse huvides vajaks vastav eesmärk täpsustamist, kuid esmalt tuleb hinnata regulatsiooni kooskõla Euroopa Liidu õigusega.

Euroopa Liidu õiguses on sideteenuste osutamise käigus kogutud isikuandmete töötlemine lahutamatult seotud õigusega eraelu puutumatusele ja isikuandmete kaitsega. Seega on asjakohane analüüsida vastavat õigust ja Euroopa Kohtu praktikat. Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi 2002/58/EÜ[151] artikli 15 lõikes 1 on sätestatud, et liikmesriigid võivad direktiivi 95/46/EÜ[152] artikli 13 lõikes 1 nimetatud valdkondade kaitseks, sh avaliku korra tagamise eesmärgil kehtestada norme, milles piiratakse nõudeid üldkasutatava

[151] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, lk 37–47; ELT eriväljaanne 13/29, lk 514–524. Muudetud Euroopa Parlamendi ja nõukogu direktiiviga 2009/136/EÜ, 25. november 2009. – ELT L 337, lk 11–36.

[152] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, lk 31–50; ELT eriväljaanne 13/15, lk 355–374.

sidevõrgu ja üldkasutatavate elektrooniliste sideteenuste kaudu toimuva side ja sellega seotud liiklusandmete konfidentsiaalsusele, kohustust kustutada sidevõrgus toimuva liikluse andmeid, kui need pole enam vajalikud side edastamiseks ja õigust välistada oma numbrinäidu edastamist. 2014. aasta lahendis *Digital Rights Ireland* tunnistas Euroopa Kohus kehtetuks direktiivi 2006/24/EÜ[153], kuna leidis, et direktiivis kavandatud meetmed on vastuolus proportsionaalsuse põhimõttega. Kohus märkis, et õigusakt peab sisaldama rakendatavate meetmete täpset ulatust ja kohaldamisala, samuti miinimumnõudeid isikuandmete kaitseks andmete kuritarvitamise ohu, ebaseadusliku juurdepääsu ja kasutamise vähendamiseks ning rõhutas, et erandid peavad piirduma rangelt vajalikuga.[154]

Täiendusena *Digital Rights Ireland* lahendile on Euroopa Kohus lahendis *Tele2 Sverige AB* tõlgendanud eelotsusetaotluse raames direktiivi 2002/58/EÜ artikli 15 lõiget 1 koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8 ning artikli 52 lõikega 1. Kohus leidis, et Euroopa Liidu õigusega on vastuolus sellised õigusnormid, mis näevad ette elektroonilise side andmete üldise säilitamiskohustuse kuritegevuse vastu võitlemise eesmärgil, tegemata vahet kõikidel liiklus- ja asukohaandmetel. Seega normid, mis reguleerivad elektroonilise side andmete kaitset ja turvalisust, sh pädevate ametiasutuste ligipääsu elektroonilise side liiklus- ja asukohaandmetele, peavad piirnema üksnes raske kuritegevuse vastu võitlemisega. Andmetele juurdepääsu üle peab Euroopa Kohtu hinnangul olema kas kohtu või haldusorgani sõltumatu kontroll ning vastavaid andmeid tuleb säilitada liidu territooriumil.[155] Kokkuvõttes nähtub Euroopa Kohtu praktikast, et pädeva korrakaitseorgani võimalused saada sideettevõtjatelt elektroonilise side liiklus- ja asukohaandmeid on tegevuse eesmärgiga võrdlemisi piiratud, olles õigustatud vaid raske kuritegevuse vastu võitlemisega. Seega sideettevõtjalt kõnealuste andmete saamine on Euroopa Liidu õiguse ja Euroopa Kohtu seisukohaga kooskõlaliselt võimalik vaid väga piiratud juhtudel. Korrakaitseõiguse kontekstis võiks see olla ohutõrje eesmärgil näiteks küberrünnaku peatamiseks. Karistusseadustikus[156] (edaspidi KarS) sätestatud süüteokoosseisud arvutiandmetesse sekkumine (KarS § 206 lg 1), arvutisüsteemi toimimise takistamine (KarS § 207 lg 1) ja arvutikelmus (KarS § 213 lg 1), on teise astme kuriteod KarS § 4 lõike 3 tähenduses. Seega eelnimetatud süütegude puhul ei saa viidata raske kuritegevusega võitlemisele, mis peaks olema aluseks sideettevõtjalt elektroonilise side liiklus- ja asukohaandmete saamisele.

[153] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. – ELT L 105, lk 54–63.
[154] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland*, p 54 ja 52.
[155] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB*, otsuse resolutsiooni p 1 ja 2.
[156] Karistusseadustik. – RT I, 26.06.2017, 8.

KorS § 35 lõike 1 sõnastusest nähtub, et korrakaitseorganil on lubatud reaalajas asukoha tuvastamist võimaldavate andmete töötlemine isiku kohta, kelle puhul tekib vajadus kõrgendatud ohu väljaselgitamiseks või ohu tõrjumiseks. Eeldusel, et kõrgendatud ohu väljaselgitamine ja tõrjumine on samastatav raske kuritegevuse vastu võitlemisega, saab sätte lugeda Euroopa Liidu õigusega kooskõlas olevaks. Eraldi küsimus puudutab aga KüTS eelnõu § 22 lõikega 5 loodavat sideettevõtja kohustust RIA-le elektroonilise side andmeid edastada. ESS-i kehtiva redaktsiooni puhul on elektroonilise side andmete säilitamises juba olemas vastuolu Euroopa Liidu õigusega ning küberturvalisuse seaduse eelnõuga plaanitakse vastuolus olevaid õiguseid veelgi laiendada, mitte kaotada. ESS-i §-s 111^1 reguleeritud andmete säilitamise korra otsese vastuolu Euroopa Liidu õigusega on välja toonud ka teised autorid. Andmete edastamist saab lugeda säilitamisest järgmiseks sammuks, kuivõrd andmete säilitamine on nende edastamise eelduseks. [157] Kuivõrd KüTS eelnõu § 22 lõike 5 sõnastusest ei nähtu, et meede oleks suunatud raske kuritegevuse vastu võitlemise eesmärgi täitmiseks, siis ilmneb kavandatava sätte puhul tõenäoline vastuolu Euroopa Liidu õigusega.

Sideettevõtjalt nõutavate andmete saamise eesmärk on tuvastada konkreetse kahjurvaraga nakatunud või sellest ohustatud seadme IP-aadress ja analüüsida seadme kaudu toimunud interneti-liiklust.[158] Küberturvalisuse seaduse eelnõu seletuskirja kohaselt isikuandmete töötlemist ei toimu, kuna IP-aadresse ei seostata nende kasutajatega.[159] Eraldi küsimus on, kas IP-aadress on käsitatav isikuandmetena. Euroopa Kohus tõlgendas lahendis *Patrick Breyer* vs *Saksamaa Liitvabariik* direktiivi 95/46 artikli 2 punkti a ning jõudis seisukohale, et juhul kui isik külastab üldiselt kättesaadavat veebilehte ja sideteenuse osutaja salvestab dünaamilise IP-aadressi, on antud kontekstis tegemist isikuandmetega, kui sideteenuse osutaja valduses oleva teabe alusel on võimalik kõnealune isik tuvastada.[160] Seega pole antud kontekstis oluline, kas IP-aadressi ka tegelikult isikuga seostatakse, vaid võimalus, et seda saab teha.

EL õigusega kooskõla saavutamiseks on advokaadibüroo SORAINEN sideandmete edastamise osas välja pakkunud kaheastmeline lahenduse: küberturvalisuse ohu ja sellega seotud asjaolude väljaselgitamine võiks toimuda isikustamata andmete põhjal. Edasi kõrgendatud ohu ilmnemise korral saaks RIA sideettevõtjalt küsida isikustatud andmed.[161] Selline lahendus järgiks Euroopa

[157] P. Schasmin, C. Ginter. Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis. – Juridica 2017/I, lk 52.
[158] Advokaadibüroo SORAINEN. Riigi Infosüsteemi Ameti järelevalve meetmed haldusjärelevalvemenetluses ning häda- ja eriolukorras, 2017. – https://www.ria.ee/public/Kuberturvalisus/Oigusanalyys-2017-Sorainen.pdf, lk 13–14.
[159] Küberturvalisuse seaduse eelnõu seletuskiri, lk 28.
[160] EKo 19.10.2016, C-582/14, *Patrick Breyer* versus *Saksamaa Liitvabariik*, p 49.
[161] Advokaadibüroo SORAINEN, lk 14–15.

Liidu õigust. Siiski ei peaks sideandmete küsimine sideettevõtjalt küberintsidendi lahendamisel olema üks põhilisi riikliku järelevalve meetmeid. Kuivõrd sideandmete kogumise ja korrakaitseorganile edastamisega on seotud Euroopa Kohtu hinnangule tuginedes intensiivne isikute põhiõiguste ja -vabaduste riive, tuleks küberturvalisuse tagamiseks võimalusel valida alternatiivsete meetmete rakendamine ning eelkõige teha intsidentide lahendamisel koostööd asjaomaste osapooltega. Proportsionaalsuse põhimõtet järgides tuleks sideandmete nõudmist kui intensiivsema riivega meedet rakendada siis, kui teised meetmed on ammendunud.

Kokkuvõttes tuleks küberturvalisuse seaduse eelnõus sätte sõnastust muuta viisil, et oleks tagatud kooskõla Euroopa Liidu õigusega või säte eelnõust välja jätta. Kuivõrd küberturvalisuse seaduse eelnõuga planeeritud sideandmete andmise kohustuse puhul ilmnes formaalõiguslik probleem, siis ei ole autori hinnangul otstarbekas meetme detailsema proportsionaalsuse analüüsiga jätkata.

3.1.10. Vallasasja läbivaatus

Vallasasja kontrollimise õigus valdaja nõusolekuta on politseil ja seaduses sätestatud juhul muul korrakaitseorganil KorS § 49 lõikes 1 nimetatud tingimustel, punkti 7 kohaselt muuhulgas kui see on pädeva korrakaitseorgani poolt vajalik seadusega või seaduse alusel kehtestatud nõuete täitmise tagamisel ohu ennetamiseks, väljaselgitamiseks, tõrjumiseks või korrarikkumise kõrvaldamiseks. Vallasasja läbivaatus on seega võimalik nii ohu ennetamise kui tõrjumise eesmärgil. RIA kui muu korrakaitseorgani volitus vallasasja läbivaatuse kohaldamiseks on sätestatud KüTS eelnõu § 16 lõikes 1. RIA pädevus on tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjaomaste punktidega. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1.

Meetme sobivuse väljaselgitamisel on esmalt asjakohane analüüsida, kas küberturvalisuse valdkonnaga seotud mõisted nagu infovara, andmekandjad ja andmesidevõrk on käsitatavad vallasasjadena või tuleks neile kohaldada muud õiguslikku režiimi. Infovara all mõistetakse KüTS eelnõu § 2 punkti 3 kohaselt informatsiooni, andmeid ja nende töötlemiseks vajalikke tehnoloogilisi rakendusi, tarkvara ning muid vahendeid. Vallasasja ja kinnisasja mõisted on defineeritud tsiviilseadustiku üldosa seaduse[162] (edaspidi TsÜS) §-s 50: lõike 1 kohaselt on kinnisasi maapinna piiritletud osa (maatükk) ja lõike 2 kohaselt loetakse vallasasjaks iga asi,

[162] Tsiviilseadustiku üldosa seadus. – RT I, 12.03.2015, 106.

mis ei ole kinnisasi. Asi on TsÜS § 49 lõike 1 kohaselt kehaline ese. Sealjuures esemeks loetakse TsÜS § 48 kohaselt asjad, õigused ja muud hüved, mis võivad olla õiguse objektiks. Andmekandjad ja tehnilised vahendid füüsilise objektina on tsiviilseadustiku üldosa seaduse tähenduses vallasasjad. Digitaalsed andmed ja virtuaalsed infovarad oleks asjakohane liigitada muude hüvede hulka, mis võivad olla õiguse objektiks ehk loetakse selles kontekstis esemeks. Kuna õigustele kohaldatakse asja kohta sätestatut TsÜS § 49 lõike 2 kohaselt, siis ka infovaradele oleks võimalik vallasasja regulatsiooni kohaldamine. Antud kontekstis oleks meetme rakendamine asjakohane näiteks pahavaraga nakatunud serveri läbivaatuseks, et selle päritolu selgitada. Õigusselguse tagamiseks oleks asjakohane küberturvalisuse seaduse eelnõus kaaluda lisaks KüTS eelnõu § 2 punktis 3 defineerimisele ka infovara õigusliku seisundi reguleerimist.

Andmesidevõrk on asjaõigusseaduse[163] (edaspidi AÕS) § 158 lõike 1 tähenduses tehnovõrk. Kuivõrd tehnovõrk pole iseseisev kinnisasi, siis tuleb hinnata, kas tegemist võib olla TsÜS § 54 lõikes 1 defineeritud kinnisasja olulise osaga. TsÜS § 54 lõikes 2 on tehtud täpsustus, et kinnisasjal paiknevat tehnovõrku või -rajatist ei loeta kinnisasja osaks, kui see on ehitatud kinnisasjale asjaõiguse alusel või selle suhtes kehtib seadusest tulenev talumiskohustus. Andmesidevõrgu puhul on seega vajalik hinnata, millisel otstarbel see on rajatud ja kellele kuulub selle omand. Sarnases küsimuses elektrialajaama kohta on Riigikohus märkinud, et elektrialajaam tuleb üldreeglina lugeda vallasasjaks TsÜS § 50 lõike 2 tähenduses. Põhjendusena lisas kohus varasemates lahendites toodud seisukoha, et seda on võimalik teisaldada ja ruumidest ära viia ilma ehitist või alajaama kahjustamata. Võrreldes üldreeglitega, siis tehnorajatiste regulatsioon laiendab võimalusi rajatise kinnisasja osaks mitte lugeda, luues võimaluse ka kinnisasja ja tehnorajatise omandite eristamiseks. Riigikohus rõhutas lahendis ka üldreegli ülimuslikkust – tehnorajatise seisund ei mõjuta alajaama õiguslikku seisundit vallas- või kinnisasjana, kui see on juba üldreegli kohaselt käsitatav vallasasjana.[164] Analoogia alusel oleks võimalik rakendada andmesidevõrgu puhul sarnast lähenemist ning käsitada ka andmesidevõrku vallasasjana.

Küberturvalisuse valdkonnas on vallasasja läbivaatus ja selles sisalduva informatsiooni kontrollimine riikliku järelevalve meetmena kasutatav selleks, et vajadusel küberintsidendiga seotud või ennetuslikult sellest ohustatud seadmes või veebikeskkonnas oleva informatsiooniga tutvuda ja vastavad asjaolud välja selgitada. Seega on meede eesmärgi suhtes sobiv näiteks

[163] Asjaõigusseadus. – RT I, 25.01.2017, 4.
[164] RKTKo 3-2-1-86-14, p 16–17, 20.

olukorras, kus seade, veebikeskkond vm on küberintsidendi poolt mõjutatud. Probleemi lahendamiseks on vaja tagada RIA kui järelevalveorgani ligipääs asjassepuutuvatele andmetele, et saada olukorrast ja edasistest arenguvõimalustest terviklik ülevaade ning vastava info põhjal kasutusele võtta vajalikud täiendavad abinõud. Meedet saab pidada vajalikuks, kuna küberintsidendi lahendamisel tõenäoliselt puuduvad alternatiivsed meetmed, mis samavõrd hästi võimaldaksid eesmärki saavutada ehk küberintsidendist tulenevat ohtu ennetada või tõrjuda.

Vallasasja läbivaatus riivab eelkõige isiku õigust omandi puutumatusele (PS § 32 lg 1 esimene lause), samuti ettevõtlusvabadusele (PS § 31 esimene lause), kuna läbivaatuse ajal on takistatud selle kasutamine valdaja poolt. Siiski puudub põhjus lugeda riivet ülemääraseks, kuna meetme kohaldamine on ajutine ega kujuta endast pikema perioodi vältel isiku õigustesse sekkumist. Teisalt on meetme rakendamine vajalik nii isiku enda kui kolmandate isikute õiguste kaitseks, et küberintsidendi võimalikke mõjusid piirata. Seega saab meetme hinnata proportsionaalseks nii ohu ennetamise kui tõrje seisukohast.

3.1.11. Valdusesse sisenemine ja valduse läbivaatus

KorS § 50 lõike 1 alusel on riikliku järelevalve erimeetmena politseil ja seadusest tuleneva volituse alusel muul korrakaitseorganil võimalik sättes nimetatud eesmärkidel siseneda piiratud või tähistatud kinnisasjale, ehitisse, ruumi või eluruumi selle valdaja nõusolekuta. KorS § 51 lõike 1 kohaselt on korrakaitseorganil õigus valdus sättes nimetatud eesmärkidel valdaja nõusolekuta ka läbi vaadata. Valdajaks loetakse AÕS § 33 lõike 1 kohaselt isikut, kelle tegeliku võimu all on asi. Valdusse sisenemisel on lubatud avada uksi, väravaid ja vajadusel kõrvaldada takistusi. Lõike 2 kohaselt on lubatud eelnimetatud tingimustel valdusesse siseneda ka madalama ohutaseme korral, kui keskmise objektiivse isiku seisukohast hinnates levivad valdusest väljapoole teist isikut oluliselt häirivad mõjutused. RIA kui muu korrakaitseorgani volitus valdusesse sisenemise ja valduse läbivaatuse kohaldamiseks on sätestatud KüTS eelnõu § 16 lõikes 1. RIA pädevus mõlema meetme kohaldamiseks on tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjaomaste punktidega. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Meetmed on rakendatavad ohutõrje eesmärgil, KorS § 50 lõike 1 punkti 3 ja KorS § 51 lõike 1 punkti 3 kohaselt ka ohu ennetamiseks.

Valdusesse sisenemisel ja läbivaatusel riikliku järelevalve erimeetmetena on seos KüTS eelnõu § 17 lõikes 1 sätestatud täiendava erimeetmega küberintsidendi tõkestamiseks. Kui KorS § 50

lõige 1 reguleerib füüsilisse valdusse sisenemist, siis KüTS eelnõu § 17 lõike 1 lause esimene pool sätestab RIA volituse riikliku järelevalve teostamisel võrgu- ja infosüsteemi juhtimise vahetult või kaughalduse teel üle võtta. Ülevõtmine on lubatud vaid sätte lõikes 2 nimetatud juhtudel koos kohustusega süsteemi haldajat teavitada ning meetme rakendamist protokollida (KüTS eelnõu § 17 lg-d 3 ja 4).

Küberturvalisuse tagamisel on RIA jaoks valdusesse sisenemiseks asjakohased kaks KorS § 50 lõikes 1 nimetatud eesmärki: vajadus välja selgitada kõrgendatud oht või see tõrjuda (KorS § 50 lg 1 p 1) ja seadusega või seaduse alusel kehtestatud nõuete täitmise tagamiseks, kui see on vajalik RIA ülesannetest tulenevalt ohu ennetamiseks, väljaselgitamiseks, tõrjumiseks või korrarikkumise kõrvaldamiseks (KorS § 50 lg 1 p 3). KorS § 50 lõike 1 punktis 2 toodud alus ei ole RIA ülesandeid silmas pidades asjakohane, kuna RIA-l puudub pädevus võtta isikult vabadus, samuti puudub ülesannete täitmiseks vajadus elu ja tervise kaitsmise eesmärgil kontrollida, kas vastaval kinnisasjal või ruumis võib viibida abitus seisundis isik. Sarnaselt valdusesse sisenemise meetmega, puudub RIA-l see pädevus ka valduse läbivaatusel (KorS § 51 lg 1). Seega meetmete sobivuse tagamise eesmärgil tuleks KüTS eelnõus nende rakendamise aluseks olevat volitusnormi täpsustada.

Kuigi nii KorS § 50 lõikes 1 kui tinglikult KüTS eelnõu § 17 lõikes 1 sätestatud meetmed puudutavad valdusesse sisenemist, on need oma olemuselt erinevad. Sisuliselt võib neid käsitada kahe eraldi etapina, sest enne võrgu- ja infosüsteemi sisenemist võib RIA-l olla vajadus siseneda KorS § 50 lõike 1 kohaselt kinnisasjale, sellel paiknevasse ehitisse või ruumi, kus vastavad seadmed ja sidevõrk asuvad, eesmärgiga rakendada näiteks vallasasja läbivaatust ründeallika tuvastamiseks. KorS § 50 lõige 1 on seotud füüsiliselt mingile alale sisenemisega.[165] Meedet ei saa samaviisi kohaldada võrgu- ja infosüsteemidesse sisenemiseks, kuna füüsiline kohalolek nendes süsteemides pole võimalik. Seega on otstarbekas valitud lähenemine ja KüTS eelnõusse § 17 lõikega 1 täiendava erimeetme lisamine, et eelkirjeldatud olukordadel vahet teha ning vältida RIA tegevuse võimalikku vaidlustamist õigusliku aluse puudumise tõttu.

Korrates eespool märgitut, võib valdusesse sisenemine osutuda vajalikuks eelduseks muude meetmete rakendamisel, eelkõige vallasasja läbivaatusel KorS § 49 lõike 1 alusel ja valduse läbivaatusel KorS § 51 lõike 1 alusel, samuti võrgu- ja infosüsteemi vahetuks ülevõtmiseks

[165] S. Pars. KorS § 50/1.

küberintsidendi tõkestamisel. Riigikohus on märkinud, et valdusesse sisenemise ja valduse läbivaatuse eesmärgid, olemus, tagajärjed ja riive intensiivsus erinevad. Valdusse sisenemise korral tuleb piirduda olukorra vaatlemisega.[166] Korrakaitseseaduse eelnõu seletuskirjas täpsustatakse, et vallasasjade läbivaatus ei ole pelgalt valdusse sisenemise meetme rakendamisel lubatud. Sellisel juhul tuleb rakendada KorS §-s 51 sätestatud valduse läbivaatust.[167] Ilma valdusse või võrgu- ja infosüsteemi sisenemiseta võivad RIA-l puududa asjakohased võimalused ohu tõrjumiseks vajalikke abinõusid rakendada, kuna vahetu viibimine küberintsidendiga seotud kohas või süsteemis võib omakorda osutuda vältimatuks eelduseks vajalikule informatsioonile ligipääsemisel.

Valdusesse sisenemine ja läbivaatus, samuti võrgu- ja infosüsteemi ülevõtmine toovad endaga tõenäoliselt kaasa omandi puutumatuse riive (PS § 32 lg 1 esimene lause). Samuti võib teatud juhtudel kaasneda kodu puutumatuse riive (PS § 33 esimene lause), kui valdusesse sisenemisest on puudutatud isiku kodu. Omandi puutumatuse puhul ei ole tegemist absoluutse õigusega – PS § 32 lõige 2 sätestab küll igaühe õiguse enda omandit vabalt vallata, kasutada ja käsutada, kuid keelab seda teha üldiste huvide vastaselt ning lubab ka vastavat õigust kitsendada seaduse alusel. Ka kodu puutumatuse osas on võimalik PS § 33 teise lause kohaselt teha reservatsioone ja vastavat põhiõigust piirata seadusega sätestatud juhtudel ja korras avaliku korra, tervise või teiste inimeste õiguste ja vabaduste kaitseks. Samuti võib valdusse sisenemine riivata perekonna- ja eraelu puutumatust ning eneseteostusvabadust (PS § 26 esimene lause, § 19 lõige 1). Ohtu ennetava eesmärgiga valdusesse sisenemine on KorS § 50 lõike 1 punkti 3 kohaselt lubatud seadusega või seaduse alusel kehtestatud nõuete täitmise tagamiseks. Kuna valdusesse sisenemise rakendamisel ei ole lubatud vallasasja läbivaatus, siis on küsitav võimalikust küberintsidendist tuleneva ohu ennetamise eesmärgil valdusesse sisenemise proportsionaalsus.

Valduse läbivaatust on vaja rakendada näiteks olukorras, kus võimalikust pahavaraga nakatumisest tuleneva ohu väljaselgitamiseks või tõrjumiseks on oluline isiku valdusest otsida seadmeid, millel võib olla seos konkreetse intsidendiga. Ainuüksi valdusse sisenemisega KorS § 50 lõike 1 alusel pole võimalik vastavat eesmärki saavutada. Valduse läbivaatus riivab õigust omandi või kodu puutumatusele veelgi enam kui valdusesse sisenemine, kuna selle eesmärk on leida üldjuhul midagi varjatut ning selle leidmiseks tuleb valduses asuvaid asju läbi vaadata ja uurida.[168] Vastava põhiõiguse teostamist on PS § 32 lõike 2 kohaselt siiski võimalik seaduse

[166] RKHKo 3-3-1-36-15, p 13.2.
[167] Korrakaitseseaduse eelnõu seletuskiri, lk 79.
[168] RKHKo 3-3-1-36-15, p 13.2.

alusel kitsendada. Suurema riive tõttu on siiski eluruumi läbivaatamise rakendamiseks riikliku järelevalve käigus vajalik asukohajärgse halduskohtu luba. Samuti on luba vaja äriruumi läbivaatamiseks väljaspool tööaega. Valdusesse sisenemise, kui väiksema riivega meetme, korral sellist luba vaja ei ole.[169] Valduse läbivaatuse rakendamine võimaldab RIA-l pädeva korrakaitseorganina vajadusel paremini küberintsidenti lahendada, kui on võimalik ligi pääseda kohale, kus ohtu kujutava tegevusega seotud seadmed asuvad. Seega saab valdusse sisenemise ja läbivaatuse järelevalve meetmetena lugeda proportsionaalseks.

Valdusesse sisenemist ja valduse läbivaatust eristavad küberturvalisuse seaduse eelnõu § 17 lõikes 1 reguleeritud küberintsidendi tõkestamisest nende kasutamise ulatus. Oma olemuselt on KorS § 50 lõike 1 alusel valdusesse sisenemine oluliselt suurema kasutusulatusega riikliku järelevalve meede, kui võrgu- ja infosüsteemi sisenemine selle ülevõtmiseks. Valdusesse sisenemine peab olema korrakaitseorgani poolt selgelt põhjendatud, kuna meetmega kaasnev põhiõiguste riive on suurem, võrreldes käesolevas töös eelnevalt analüüsitud meetmetega. KüTS eelnõu § 17 lõikes 1 sätestatud erimeetme kohta on eelnõu koostajad märkinud, et see on ette nähtud kiire reageerimise vajadusega juhtumite korral. Üheks taoliseks näiteks, kus ohustatud on inimelud, -tervis, vara või avalik kord laiemalt, on kriitilise infrastruktuuri, sh oluliste võrgu- ja infosüsteemide ründamine. Kui intsidendi võimalikud mõjud on väga ulatuslikud ja päevakorral on niivõrd kaalukate õiguste tagamine nagu inimeste elu ja tervise kaitse, kaalub eesmärgi olulisus üle põhiõiguste riive ning meetme saab lugeda mõõdukaks. Kokkuvõttes on mõlemad meetmed sobivad eesmärkide saavutamiseks. Siiski vajaks autori hinnangul täpsustamist KüTS eelnõu § 17 lõikes 1 sätestatud volitusnorm (vt jaotis 3.1.4.).

Kaalumist vajaks täiendavalt ka võrgu- ja infosüsteemi sisenemise ja läbivaatuse õiguse sätestamine küberturvalisuse seaduse eelnõus. Eelnõus on sätestatud RIA-le volitusnorm valdusesse sisenemiseks ja selle läbivaatuseks, kuid sarnaseid meetmeid ei ole sõnastatud võrgu- ja infosüsteemi kohta. Kuna võrgu- ja infosüsteemi sisenemine ja selle läbivaatus ei ole samasisulised tegevused, mis füüsilisse valdusse sisenemine ja läbivaatus, võib viimasest RIA-le küberturvalisuse tagamise eesmärgil jääda väheks. KüTS eelnõu § 17 lõike 1 kohaselt võib RIA võrgu- ja infosüsteemi juhtimise vahetult või kaughalduse teel üle võtta ja selle kasutamist või juurdepääsu piirata, kui see on vajalik kõrgendatud ohu või selle kahtluse korral. Seega vajab autori hinnangul kaalumist selgesõnalise volituse sätestamine süsteemi sisenemiseks ja läbivaatuseks juhtudeks, kui selle ülevõtmine pole vajalik.

[169] S. Pars. KorS § 51/1, 4.

3.1.12. Vallasasja hoiulevõtmine

Politseil ja seaduses sätestatud juhul muul korrakaitseorganil on KorS § 52 lõike 1 alusel ja sättes nimetatud eesmärkidel õigus võtta vallasasi hoiule. RIA kui muu korrakaitseorgani volitus vallaasja hoiulevõtmiseks on sätestatud KüTS eelnõu § 16 lõikes 2. RIA võib kohaldada vastavat erimeedet riikliku järelevalve teostamisel teenuse osutajate üle, kes on kohustatud järgima KüTS eelnõu §-des 7 ja 8 sätestatud nõuete täitmist. Meedet kohaldatakse lisaks muudele erimeetmetele, mis on nimetatud KüTS eelnõu § 16 lõikes 1. RIA pädevus vallasasja hoiulevõtmisel on tuletatav asutuse põhimääruse § 8 punktist 1 koosmõjus § 9 asjaomaste punktidega. Lisaks on üldine pädevusnorm sõnastatud KüTS eelnõu § 13 lõikes 1. Meede on rakendatav ohutõrje eesmärgil.

KorS § 52 lõikes 1 on nimetatud kokku 5 alust, milleks on vallasasja hoiulevõtmine õigustatud. Meetme sobivust hinnates ei ole kõik nimetatud eesmärgid RIA läbiviidava riikliku järelevalve kontekstis asjakohased. Küberturvalisuse tagamisel on vallasasja hoiulevõtmine eelkõige sobiv ja vajalik küberintsidendist tuleneva vahetu ohu tõrjumiseks või korrarikkumise kõrvaldamiseks. Samuti võib meede asjakohaseks osutuda vallasasja mõõtmiste või ekspertiisi teostamiseks, näiteks pahavara levimisega seotud serveris sisalduvast informatsioonist tõmmise tegemiseks edasise analüüsimise eesmärgil. Sättes nimetatud teiste aluste seos RIA ülesannete täitmisega ja vajadus küberturvalisuse valdkonnas rakendada jääb autori hinnangul ebamääraseks. Ka küberturvalisuse seaduse eelnõu seletuskiri ei sisalda selle kohta infot. Meetme sobivuse tagamiseks tuleks küberturvalisuse seaduse eelnõus täpsustada volitusnormi ja nimetada konkreetsed alused, milleks RIA on õigustatud vallasasja hoiule võtma.

Vallasasja hoiulevõtmine riivab sarnaselt käesolevas töös eelnevalt analüüsitud riikliku järelevalve meetmetele PS § 32 lõike 1 esimesest lausest tulenevat õigust omandi puutumatusele. Meetme rakendamisega kaasnev riive on intensiivsem kui pelgalt vallasasja või valduse läbivaatuse korral, kuna asja valdaja jääb selle kasutuseelistest vähemalt ajutiselt ilma. Seega peaks RIA konkreetses olukorras korrakaitseorganina veenduma, et vallasasja hoiulevõtmisega on tagatud meetme rakendamise vahetu eesmärk, sh küberintsidendist tuleneva vahetu ohu tõrjumine või korrarikkumise kõrvaldamine. Üldjoontes saab aga ka seda meedet pidada küberturvalisuse valdkonnas rakendamiseks proportsionaalseks.

3.1.13. Muu meede – nn virtuaalne viibimiskeeld

Küberturvalisuse valdkonnas oleks autori hinnangul asjakohane analüüsida ka riikliku järelevalve erimeetmena nn virtuaalse viibimiskeelu rakendamist. Lisaks võrgu- ja infosüsteemi turvalisuse ohustamisele võib pahatahtlik kübertegevus kätkeda endas ohuallikat ka interneti kasutajate elule ja tervisele. Eesmärk on piirata juurdepääsu teatud veebikeskkonnale või -teenusele, näiteks takistades kasutajate ligipääsu ebaseaduslikule veebisisule olukorras, kus tegemist ei ole küberintsidendiga. Küberturvalisuse seaduse eelnõus on võrgu- ja infosüsteemi turvalisus ja seda ohustav küberintsident defineeritud kitsalt ning selline tegevus termini alla ei paigutu. Meetme kohaldamise vajadus võib tekkida ka küberintsidendi ohu korral, näiteks aegunud operatsioonisüsteemide kasutajate võrgukasutuse piiramiseks olukorras, kus operatsioonisüsteemide haavatavust kasutatakse lunavara levitamiseks. Asjaomane näide on alapeatükis 2.1. käsitletud lunavara rünnak WannaCry.

Korrakaitseseadus küberturvalisuse valdkonna jaoks sobivat meedet ei sisalda. KorS § 44 lõike 1 alusel saab küll viibimiskeeldu riikliku järelevalve erimeetmena politsei ning seaduses sätestatud juhul ka muu korrakaitseorgan ajutiselt rakendada. Kuid meetme sisu seisneb isiku füüsilise viibimise keelamises teatud isiku läheduses või kohas, samuti tema kohustamises lähenemisest hoiduma või lahkuma isiku elu või tervist ähvardava vahetu ohu korral, ülekaaluka avaliku huvi kaitseks, kõrgendatud ohu väljaselgitamiseks või tõrjumiseks, kaitstava isiku või valvatava objekti ohutuse tagamiseks, süüteomenetluse läbiviimise tagamiseks või riikliku järelevalve meetme kohaldamise tagamiseks. KorS § 44 lõike 1 tähenduses saab viibimiskeelu anda konkreetse koha suhtes. Koha all mõistetakse maa-ala, ehitist või rajatist, mille suhtes rakendatakse keeldu seal viibida ning kust isikud kohustatakse lahkuma.[170] Ka virtuaalse keskkonna tähenduses saame rääkida viibimiskohast, kuna iga veebileht kannab unikaalset aadressi. Siiski ei võimalda KorS § 44 lõike 1 tõlgendamine asuda seisukohale, et koha mõiste laieneb ka interneti-keskkonnale, kuna säte viitab selgelt füüsilisele viibimiskohale. Küberturvalisuse seaduse eelnõus sätestatud erimeetme kohaselt saab RIA küll võrgu- ja infosüsteemi kasutamist või sellele juurdepääsu piirata (KüTS eelnõu § 17 lõige 1). Kuid meede on kohaldatav vaid küberintsidendi tõkestamiseks: KüTS eelnõu § 17 lõike 1 teises pooles on sätestatud RIA-le õigus süsteemi kasutamist või süsteemile juurdepääsu piirata küberintsidendist põhjustatud kõrgendatud ohu väljaselgitamiseks või tõrjumiseks. Seega eelkirjeldatud olukorras meede kohaldamisele ei tuleks, kuna tegemist pole küberintsidendiga. HOS § 33 lõike 2 alusel on eriolukorra juhil õigus kohustada elutähtsa teenuse osutajat piirama

[170] Korrakaitseseaduse eelnõu seletuskiri, lk 85.

lõppkasutajate võimalust kasutada teenust või sidevõrku eriolukorra väljakuulutamise põhjustanud hädaolukorra lahendamiseks. Vastav volitusnorm ei anna aga alust meedet kohaldada ilma eriolukorda väljakuulutamata.

Teatud võimalused seadusvastasele informatsioonile ligipääsu piiramiseks internetis annab infoühiskonna teenuse seadus[171] (edaspidi InfoTS): infoühiskonna teenuse piiramine on õigustatud kõlbluse, avaliku korra, riigi julgeoleku, rahva tervise ja tarbija kaitseks (InfoTS § 3 lg 2), kui see vastab sättes nimetatud tingimustele (InfoTS § 3 lg 3). Piirangu rakendamine küberturvalisuse tagamiseks on siiski problemaatiline, kuna infoühiskonna teenuse seaduse kohaselt on piirangu seadmise olemus ja ulatus abstraktsed.[172] Samuti ei nimeta seadus piirangu seadmiseks pädevat asutust, mistõttu infoühiskonna teenuste piiramine eelnimetatud alustel on muu organi puudumisel politsei pädevuses KorS § 6 lõike 2 alusel. Üks võimalik lahendus on infoühiskonna teenuse seaduse täiendamine piirangu rakendamise võimaluste täpsustamiseks, sh kaaluda asjakohasele korrakaitseorganile vastava volitusnormi sätestamist. Meedet rakendav korrakaitseorgan võiks olla RIA, kelle üldine pädevus virtuaalses keskkonnas viibimise piiramiseks on seotud küberturvalisuse tagamise ülesandega (KüTS eelnõu § 13 lõige 1). Volitusnormi sätestamisel tuleks lisada vastav pädevus ka RIA põhimäärusesse.

Meede oleks sobiv näiteks olukorras, kus veebilehel kutsutakse teismelisi üles ennast või teisi vigastama või surmama (nn surmamängud). Riikliku järelevalve korras peaks olema võimalik selliste veebilehtede kasutamist piirata. Ohtlikule veebisisule ligipääsemiseks on tehniliselt võimalik näiteks Eesti maatunnusega IP-aadressi põhiselt keelata teatud aadresside külastamine. Meetme vajalikkus on päevakorral eelkõige seoses sellega, et internetist tulenevatest ohtudest teavitamine ei osutu sageli piisavalt mõjusaks meetmeks ning vähemalt ajutine ligipääsu piiramine aitaks konkreetse olukorraga seotud riske maandada. Üldine võrgu- ja infosüsteemi kasutamise või juurdepääsu piirang osutuks eesmärki arvestades ülemäära kolmandate isikute õiguseid riivavaks. InfoTS täiendamist võiks kaaluda inimeste elu ja tervise kaitse eesmärgil, et RIA-l oleks võimalik teha teenuse osutajale ettekirjutus konkreetsele veebilehele ligipääsu piiramiseks.

[171] Infoühiskonna teenuse seadus. – RT I, 12.07.2014, 48.
[172] Vt infoühiskonna teenuse seaduse analüüsi, koostaja M. Gross. Käesolevas töös ei ole analüüsi olemasolul infoühiskonna teenuste piiramist detailsemalt käsitletud. Allikas: Eesti Vabariigi Justiitsministeerium. Meediateenuste ja sideteenuste piiramine avaliku julgeoleku ja avaliku korra kaitseks. Justiitsministeerium: 2017 (analüüsi väljavõte autori valduses, analüüs Justiitsministeeriumi valduses).

Virtuaalse viibimiskeelu rakendamisel tuleb arvestada märkimisväärse riivega PS § 44 lõikest 1 tuleneva õiguse suhtes vabalt saada üldiseks kasutamiseks levitatavat informatsiooni. Sisuliselt on tegemist informatsiooniga, mis on antud avalikku teabelevisse. Normi kaitsealasse kuuluvad igasugused teabeallikad, mille vahendusel on igal isikul võimalik saada talle huvipakkuvat teavet. Kuna õigust informatsioonile on võimalik sisustada küllaltki avaralt, siis peab vastav põhiõigus olema ka laialt kasutatav. Tegemist on reservatsioonita põhiõigusega, seega piirang peab olema õigustatav muude põhiõiguste kaitsega. PS § 45 teise lause kohaselt võib seadus seda õigust piirata avaliku korra, kõlbluse, teiste inimeste õiguste ja vabaduste, tervise, au ning hea nime kaitseks. Seetõttu tuleks korrakaitseorganil veebilehe sisu enne meetme rakendamist põhjalikult hinnata ning meetme kasutamist argumenteerida. PS § 44 lõige 1 hõlmab endas nii tõrjeõigust, mis kujutab avaliku võimu kohustust hoiduda avalikustatud teabele juurdepääsu takistamast või muul moel sekkumast. Siia alla saab paigutada ka välismaalt tuleva info leviku ja veebilehtedele juurdepääsu piiramise, mis oma olemuselt on intensiivne riive. Vähem riivav on riigivõimu positiivne õigus ise avalikes huvides ja põhiõiguste kaitseks teavet avaldada ja kohustada eraõiguslikke isikuid seda tegema.[173] Alternatiivne võimalus ligipääsu piiramisele on ohustavate veebikeskkondade tähistamine.

Kokkuvõttes saab avaliku korra, elu ja tervise kaitse jm asjakohastel eesmärkidel internetile ligipääsu piiramist pidada mõõdukaks meetmeks. Piirangu eesmärk on kaitsta selliseid õiguseid, mis kaaluvad üles õiguse saada ligi igasugusele levitatavale informatsioonile, muuhulgas mille olemust ja ohtlikkust ei pruugi selle tarbijad osata täpselt hinnata. Kuna meetme rakendamisega kaasnev riive oleks intensiivne, saaks seda rakendada *ultima ratio* põhimõttel, kui muud meetmed ei osutu piisavaks ning selleks on selge ja põhjendatud vajadus. Analüüsitud tingimustel saab autori hinnangul nn virtuaalset viibimiskeeldu pidada põhiseadusega kooskõlas olevaks.

3.2. Järeldused ja küberturvalisuse valdkonna õigusloome edasised väljakutsed

Mitmed ettepanekud küberturvalisuse seaduse eelnõu täiendamiseks esitas autor käesoleva töö eelnevates jaotistes, kus see oli asjakohane. Käesolevas alapeatükis lisab autor täiendavad järeldused ja tähelepanekud.

Floridi näeb info- ja kommunikatsioonitehnoloogia levikus informatsiooni revolutsiooni, mis seisneb küberruumi kui uue füüsilise ja intellektuaalse ruumi ülesehitamises ja millega

[173] N. Parrest, E. Vene. PõhiS § 44/9, 11–16.

kaasnevad ühiskonnas suured muutused. Üks käsitluse põhiküsimusi seisneb selles, mis on reaalsus. Küberruum on muutunud osaks igapäevasest reaalsusest – virtuaalsel kujul olev on ka teatud mõttes reaalne. Küberruumi jaoks on vaja luua eetilist raamistikku, mis arvestaks selle toimimise reegleid ning võimaldaks tulevikus lahendada senitundmatuid probleeme.[174] Autor leiab, et sarnaselt eetilisele raamistikule, mida küll siinses töös ei käsitleta, on vajadus ka tervikliku õigusliku raamistiku järele.

Küberturvalisuse seaduse eelnõuga on küberturvalisuse valdkonna reguleerimisel Eestis kahtlemata edasi liigutud. Peamine probleemkoht on siiski asjaolu, et eelnõu ning selle seletuskirja põhjal ilmneb, et endiselt puudub valdkonna õigusliku raamistiku osas terviklik vaade. Ohtudega toimetulekuks on riigis vaja kujundada selge arusaam, kuidas on võimalik küberruumis turvalisust tagada ning kehtestada selleks vajalik õiguslik raamistik. Sealhulgas on oluline õigusloome planeerimisel analüüsida, milliseid meetmeid on iga konkreetse ohu – antud juhul küberturvalisust ohustava suundumuse ja küberintsidendi liigi – korral võimalik ja asjakohane rakendada. Autori hinnangul ei peaks eesmärgiks seadma, et tulevikus küberturvalisuse tagamist reguleerida ilmtingimata ühe valdkondliku seadusega. Kuna tegemist on horisontaalse valdkonnaga, siis küberturvalisuse seaduse eelnõu peaks koos teiste seadustega moodustama ühtse ja läbimõeldud kogumi küberturvalisuse tagamiseks kehtestatud õigusest. Küberruumis turvalisuse tagamiseks ei piisa üksnes ohtude ennetamisest ja tõrjumisest korrakaitseõiguse kontekstis. Oluline roll on ka isikuandmete kaitse, infosüsteemide turvameetmete alastel jm asjakohastel regulatsioonidel. Riigi kasutatavate meetmete valik peaks tuginema ohtude analüüsile ja sellest tulenevalt kujundama õiguslikku raamistikku, mis koos muude meetmetega moodustab turvalise infoühiskonna planeerimise kava.[175]

Küberturvalisuse seaduse eelnõus reguleeritakse peaasjalikult võrgu- ja infosüsteemide kaitset ehk infrastruktuuri turvalisuse tagamiseks võetavaid meetmeid. Peamine eesmärk peaks olema siiski selle kasutajate kaitse, sh vaba ja turvalise ligipääsu tagamine informatsioonile. Eelnõu ettevalmistamisel kaaluti pealkirjana võrgu- ja infosüsteemi turvalisuse seadust, mis olnuks asjakohasem, kuna peegeldab praegust eelnõu sisu täpsemini. Samuti keskendub seadusega ülevõetav NIS direktiiv võrgu- ja infosüsteemide turvalisusele. Hea õigusloome ja normitehnika eeskirja[176] § 21 lg 1 kohaselt peab seaduseelnõu pealkiri võimalikult lühikeses

[174] L. Floridi. The ethics of information. Oxford: Oxford University Press, 2013, lk 17–18.
[175] E. Tikk, A. Nõmper, lk 168–173.
[176] Hea õigusloome ja normitehnika eeskiri. VVm 22.12.2011 nr 180. – RT I, 29.12.2011, 228.

üldistavas sõnastuses väljendama eelnõu reguleerimisala.[177] Autori hinnangul vääriks küberturvalisuse tagamine reguleerimisesemena praeguse kitsa tehnoloogiakeskse vaate asemel siiski laiemat lähenemist. Sellele viitab ka erinevate ametkondade raportite põhjal kujunenud pilt valdkonda ohustavatest suundumustest. Siinkohal väärib kordamist eelnevas analüüsis toodud ettepanek täpsustada küberturvalisuse sisu. Ka selgus eelnevas analüüsis, et küberturvalisuse seaduses puudub küberintsidendi mõistel selge seos korrarikkumise mõistega, kuigi eelnõu sisu tõlgendades on võimalik seda järeldada. Avaliku korra kaitset reguleerivas õiguses on keskne akt korrakaitseseadus – kuna see moodustab koos eriseadustega korrakaitse õigusliku terviku, tuleb küberturvalisuse seaduse eelnõu, kui eriseaduse, loogika ja terminoloogia viia vastavusse korrakaitseseadusega.

Küberturvalisuse seaduse eelnõu üks eesmärke on reguleerida alused ohtude ennetamiseks, väljaselgitamiseks ning tõrjumiseks küberruumis, sätestades RIA pädevuse riikliku ja haldusjärelevalve teostamisel.[178] Käesolevas analüüsis selgus, et korrakaitseõiguse põhine lähenemine ei ole ammendav kõikide küberturvalisust ohustavate probleemidega toimetulekuks. Samuti ei ole eelnõu koostamisel põhjalikult analüüsitud kübeturvalisuse valdkonnas riikliku järelevalve meetmete rakendamisega kaasneva riive kooskõla põhiseadusega. Eelnõu seletuskirjas märgitakse, et küberruumi reguleeriva õiguse põhjalikum analüüs on tegemata ajapuuduse tõttu, kuna küberturvalisuse seaduse eelnõu ettevalmistamine on seotud NIS direktiivi ülevõtmisega, mille tähtaeg on 9. mai 2018.[179] Kõnesolev direktiiv sätestab Euroopa Liidu liikmesriikidele kohustuse reguleerida turvameetmete rakendamise ja teavitamise nõuded olulise teenuse ja digitaalse teenuse osutajatele. Kuivõrd eelnõu on tihedalt seotud direktiivi ülevõtmise kohustusega, on selle sisu olemasoleval kujul peamiselt rahvusvahelise õiguse peegeldus. Seetõttu on kaheldav, kas küberturvalisuse seaduse eelnõu täidab piisavas ulatuses oma eesmärki riigisisese reguleerimise seisukohast, sest muuhulgas mitmed käesolevas töös markeeritud probleemid on jäänud eelnõuga lahendamata.

Kuna ajapuudusel on küberturvalisuse valdkonna reguleerimise mõjuanalüüs tegemata, on asjakohane uuesti pöörduda sissejuhatuses püstitatud ülesande juurde ja küsida, kuidas see puudutab isikute põhiõiguste ja -vabaduste kaitse tagamist. Kuigi lõpliku vastuse annab meetme kohaldamise kaalumine konkreetses olukorras, peaks seadusandja olema veendunud, et seaduse vastuvõtmisega on õiguste kaitsmiseks olemas piisavad alused. Eelnõu seletuskiri peaks andma

[177] Vt eelnõu ametlikul kooskõlastamisel esitatud märkuseid küberturvalisuse seaduse eelnõu seletuskirja lisas 3 esitatud kooskõlastustabelis. Materjalid on kättesaadavad eelnõude infosüsteemis.
[178] Küberturvalisuse seaduse eelnõu seletuskiri, lk 2.
[179] Sama, lk 3.

piisavalt põhjalikku informatsiooni, milleks konkreetseid riikliku järelevalve meetmeid vaja läheb ning kuidas nende rakendamine mõjutab õiguste kandjat. Kuigi eelnõu üks eesmärke on riikliku järelevalve meetmete täpsustamine, ei anna seletuskiri vastust, kas ja millises ulatuses on planeeritavate järelevalvemeetmete rakendamine põhiseadusega kooskõlas. Eelnõu autorid märgivad selgitusena lakooniliselt, et NIS direktiivi eesmärkide elluviimiseks „/…/ on eelnõus sätestatud järelevalvemeetmed põhjendatud ja kohased, et sekkuda võrgu- ja infosüsteemi turvalisust ähvardava või realiseerunud ohu korral ohu väljaselgitamiseks või tõrjumiseks proportsionaalsel viisil, vältides ohu süvenemist või laienemist teistele süsteemidele.“[180] Euroopa Liidu õigusest tuleneb küll liikmesriikide kohustus küberturvalisust tagada ja selleks järelevalvemeetmeid rakendada, kuid eesmärgi saavutamiseks rakendatavate meetmete valik peaks tuginema analüüsile ja olema selgemalt põhjendatud, kuna tegevusega kaasneb isikute põhiõiguste riive. Oluline on eristada ohu ennetamiseks ja tõrjumiseks rakendatavaid meetmeid – esimese puhul peab riive olema eriti põhjendatud. Seda täpsemini tuleb hinnata, kui kaugele on võimalik põhiõiguste ja -vabaduste piiramisega minna, et õigushüvede kahjustamise ennetamine ei muutuks tegude ennustamiseks, mis väljub riikliku järelevalve piiridest. Seetõttu teatud meetmeid ei ole lubatud ohu ennetamise eesmärgil kasutada. Osadel juhtudel on otstarbekuse küsimus, kas meedet peaks rakendama ohu ennetamise või tõrjumise eesmärgil. Seletuskirjast ei selgu, et meetmete planeerimisel oleks neid aspekte põhjalikumalt analüüsitud. Õigusloome põhjendamise kohustusse kergekäeline suhtumine ohustada ka demokraatlikku riigikorda üldiselt, kui puudub ülevaade, millised tagajärjed kaasnevad riigi tegevusega.

Põhiseaduses reguleeritud põhiõigused ja -vabadused on olemuselt universaalsed ja seega küberruumis kohalduvad. Sama kehtib ka õiguste piiramise kohta – see on küberruumis lubatud teiste põhiseaduslikku järku väärtuste kaitseks ning peab olema igakordselt põhjendatud. Autor nõustub töö esimeses peatükis viidatud van Kempeni seisukohaga, et käsitletud eesmärgid – turvalisus ning põhiõiguste ja -vabaduste kaitse – pole alati vastandlikud. Siiski võivad need osutuda omavahel konkureerivaks, sest kõiki hüvesid pole võimalik alati tagada nii, et ei peaks mõnest hüvest loobuma. Riikliku järelevalve teostamine peab olema põhiseadusega kooskõlas, mis tähendab, et vastavate piiravate meetmete rakendamisel tuleb arvestada põhiõiguste ja -vabaduste tagamisega. Siin tõusetub küsimus, kas õigused ja vabadused küberruumis peaksid olema samasugused kui muus avalikus ruumis. Korrakaitseõiguse loogika kohaldamine küberturvalisuse valdkonnas tugineb eeldusele, et küberruum moodustab osa avalikust ruumist, seega tuleks ka küberruumis kehtivaid õiguseid ja vabadusi sarnaselt käsitleda. Kahtlemata

[180] Küberturvalisuse seaduse eelnõu seletuskiri, lk 3.

muudab küberturvalisuse alase reguleerimise keeruliseks tehnoloogia arengu kiirus ja küberruumi globaalsus. Seetõttu tuleb tõenäoliselt aktsepteerida teatud ulatuses õigustest ja vabadustest loobumist küberruumist tulenevate ohtudega toimetulekuks ja ühiskonna turvalisuse tagamiseks. Autori hinnangul on oluline tasakaalu leidmine, mille keskmes on inimeste, mitte tehnoloogia turvalisus. Seda enam on oluline põhjendamine, miks riik on teinud valiku konkreetses situatsioonis meetmeid rakendada.

KOKKUVÕTE

Küberruumiga on seotud lai spekter erinevaid ohtusid, mis sageli on riikideülese loomuga. Kuigi küberturvalisuse tagamisel on oluline roll rahvusvahelisel õigusel, on ohtudega toimetulekuks vaja reguleerida ka asjakohased riigisisesed meetmed. Eestis on selleks valitud korrakaitseõigusel põhinev lähenemine ja vastavate riikliku järelevalve erimeetmete rakendamise volitusnormid sätestatakse küberturvalisuse seaduse eelnõus. Julgeoleku ja avaliku korra kaitsmine ning isikute põhiõiguste ja -vabaduste tagamine on kõik põhiseaduslikku järkku väärtused, kuid kaitsekohustuse täitmisel võib nende vahel tekkida konkurents, mis tingib vajaduse õiguste riiveks. Õiguspärane on riive, mis on põhiseadusega ja vastava õiguse olemusega kooskõlas ning vajalik. Analüüsist järeldus, et küberruumis turvalisuse tagamine on sisuliselt seotud avaliku korra tagamisega, mis on eelkõige riigi pädevuses. Seega Eesti õiguskorra ülesehitust arvestades on asjakohane küberruumis kohaldada ohtude ennetamiseks ja tõrjumiseks riikliku järelevalve meetmeid. Küberruum omab võrreldes füüsilise keskkonnaga erisusi, kuid korrakaitseõigus võimaldab ka selles valdkonnas meetmeid kujundada valdkonnast tulenevate erisustega ning tagada sealjuures ka subjekti õiguste kaitse.

Käesoleva magistritöö eesmärk oli anda ülevaade Eestile mõju avaldavatest küberohtudest ning leida vastus, kas küberruumis turvalisuse tagamisel on õigussubjektide põhiõiguste ja -vabaduste teostamise võimalus kaitstud. Töö fookuses oli küberturvalisuse seaduse eelnõuga planeeritavate riikliku järelevalve meetmete rakendamisega kaasnev põhiõiguste ja -vabaduste riive. Magistritööga püstitatud eesmärk sai täidetud ja peamised järeldused on esitatud alljärgnevalt. Hinnati, millises ulatuses on küberturvalisuse seaduse eelnõu alusel RIA rakendatavate riikliku järelevalve meetmete planeerimisel järgitud põhiõiguste ja -vabaduste kaitse kohustust kooskõlas põhiseadusega. Analüüsi vahendiks oli Riigikohtu poolt tunnustatud proportsionaalsuse test, hindamaks sekkumismeetmete sobivust, vajalikkust ja mõõdukust. Autor püstitas hüpoteesi, mille kohaselt on Eestis küberruumis turvalisuse tagamiseks planeeritud ulatuslikud riikliku järelevalve meetmed, kuid kaasnev põhiõiguste ja -vabaduste riive pole kõigi meetmete puhul eesmärgi suhtes proportsionaalne.

Koondjäreldusena märgib autor, et hüpotees leidis kinnitust. Küberturvalisuse seaduse eelnõuga laiendatakse RIA volitusi riikliku järelevalve erimeetmete rakendamisel, mille tulemusel saab amet kasutada ulatuslikke riikliku järelevalve meetmeid küberturvalisuse tagamiseks. Pädevused ja volitused riikliku järelevalve üldmeetmete rakendamiseks olid RIA-l korrakaitseorganina väiksemas ulatuses ka enne kõnesoleva eelnõu ettevalmistamist. Selleks, et riigi rakendatavad meetmed oleksid tulemuslikud, tuleb nende planeerimisel kujundada selge

arusaam, milliste probleemide lahendamiseks on neid vaja. Kuigi analüüsitud riikliku järelevalve meetmed olid toodud kitsendustega küberturvalisuse tagamise eesmärgil põhiseadusega kooskõlas, leidis kinnitust, et põhiõiguste ja -vabaduste riive pole kõigi meetmete puhul piisavalt selgelt tuvastatud ja põhjendatud. Mitmed riikliku järelevalve meetmed tuleks küberturvalisuse seaduse eelnõus detailsemalt reguleerida või vähemalt seletuskirjas meetme rakendamisega kaasnevat riivet detailsemalt analüüsida.

Hüpoteesi kontrollimiseks püstitati kolm uurimisküsimust. Esimene uurimisküsimus puudutas Eestile küberruumis avalduvaid ohtusid ja vastavalt kohaldatavat õigust. Nii välisorganisatsioonide kui Eesti ametkondade koostatud analüüsid kinnitasid nn ohupildi mitmekülgsust, alates küberkuritegevusest kuni riigi suveräänsusesse sõjalise sekkumise ohuni. Sõltuvalt probleemi olemusest tuleb kohaldamisele kas riigisisene või rahvusvaheline õigus. Arvestades küberruumis esinevate ohustavate suundumuste olemust, tuleb küberturvalisust käsitada laiemalt, kui kõnesolev eelnõu seda teeb. Lisaks riikliku järelevalve meetmetele rakendatakse küberturvalisuse tagamise eesmärgil ka muid asjakohaseid meetmeid, sh andmekaitse-, infoturbe- ja ka mitteregulatiivseid meetmeid. Korrakaitseõiguse põhine lähenemine on käsitletud küberturvalisust ohustavatest suundumustest asjakohane küberkuritegevuse vastase võitluse ja elutähtsate teenuste toimepidevuse tagamise, lisaks osaliselt ka terrorismi ning küberspionaaži vastase võitluse eesmärgil. Lisaks tuleb arvestada, et küberintsidentide ennetamine ja tõrjumine tugineb eeldusele, et küberintsidenti käsitatakse korrakaitseõiguse kontekstis korrarikkumisena. Vastav asjaolu küberturvalisuse seaduse eelnõust siiski otsesõnu ei selgu.

Teine uurimisküsimus puudutas küberturvalisuse tagamise eesmärgil olemasolevate ja planeeritavate riikliku järelevalve meetmete kooskõla põhiseadusega. Analüüsi fookus oli seatud riikliku järelevalve meetmete rakendamisel põhiõiguste ja -vabaduste kaitse tagamisele. Kokku analüüsiti 11-s korrakaitseseaduse paragrahvis reguleeritud riiklikku järelevalve meetmeid, mida on RIA-l võimalik küberturvalisuse tagamiseks kohaldada korrakaitseseadusest tuleneva üldvolituse või küberturvalisuse seadusega planeeritava erivolituse alusel. Meetmeid analüüsiti ükshaaval, sh ka osade kaupa, või mitut meedet koos, kus see oli asjakohane. Meetme proportsionaalsuse hindamisel eristati, kas seda tehakse ohu ennetamise või ohu tõrjumise eesmärgil – ohu ennetamiseks kohaldatavate meetmete ulatus on isikute õigustesse ja vabadustesse sekkumisel piiratum ning peab olema enam põhjendatum. Tuvastati, et kõnesoleva eelnõuga kaasneb eelkõige ettevõtlusvabaduse, eraelu ja kodu puutumatuse, isikupuutumatuse, omandiõiguse ning üldise vabaduspõhiõiguse riive.

Ühtegi põhiseadusega otseses vastuolus olevat riikliku järelevalve meedet analüüsi käigus ei tuvastatud. Samas polnud ka ühtegi meedet, millega seoses poleks tuvastatud põhiõiguste- ja vabaduste riive seisukohast probleeme, sh peamiselt puudusi meetmete põhjendatuses. Küberturvalisuse seaduse eelnõu seletuskirjast ilmnes, et meetmete proportsionaalsust on väga üldsõnaliselt analüüsitud. Kuigi käesolev töö seda ülesannet täidab, rõhutab autor, et tulenevalt suurest abstraktsiooniastmest pole ka siinne analüüs ammendav. Lõpliku vastuse iga meetme proportsionaalsuse kohta saab anda siiski konkreetses kontekstis igakordselt olukorra asjaolusid analüüsides. Võrreldes teiste meetmetega ilmnes see eriti vahetu sunni, sundtoomise, isikusamasuse tuvastamise ja küberintsidendi ennetamise eesmärgil valdusesse sisenemise puhul. Nimetatud meetmete puhul on korrakaitseorgan piiratud analüüsis käsitletud lisatingimustega, et kaasnevat riivet saaks pidada põhiseadusega kooskõlas olevaks. Autor tõi täiendava järeldusena välja, et proportsionaalsuse põhimõtet järgides ei peaks osa riikliku järelevalve meetmeid olema esimeses järjekorras kohaldatavad. See tähendab, et riikliku järelevalve teostamisel tuleks esmalt eelistada vähem koormavamaid meetmeid ja alles nende ammendumisel rakendada selliseid meetmeid, mis koormavad subjekti rohkem. Vastavad subjekti rohkem koormavad meetmed olid lisaks sunnivahenditele ka küberintsidendi tõkestamine ja võimaliku täiendava meetmena nn virtuaalse viibimiskeelu kohaldamine. Põhjendatud oleks arvata sellesse loetellu ka isikuandmete saamine sideettevõtjalt, kuid esmajoones vajaks lahendamist sellega seotud formaalõiguslik probleem – küberturvalisuse tagamise eesmärgil on meede Euroopa Liidu õigusega tõenäoliselt vastuolus. Isikuandmete saamine saab olla Euroopa Kohtu hinnangule tuginedes proportsionaalne vaid raske kuritegevuse vastu võitlemise eesmärgil. Kuna see eelnõu sõnastusest ei selgu, tegi autor ettepaneku täpsustada küberturvalisuse seaduse eelnõus vastava sätte sõnastust või alternatiivse lahendusena meetmest loobuda.

Viimane uurimisküsimus puudutas täiendavate piiravate meetmete kehtestamise vajadust. Kuigi analüüsi tulemusel ei selgunud vajadust ühegi uue meetme järgi, tuleks kaaluda küberturvalisuse seaduse eelnõu täpsustamist. Autor tegi ettepaneku täiendada asjaomaseid meetmeid ettekirjutuse tegemiseks väljaspool hädaolukorda ohtu ennetaval eesmärgil, võrgu- ja infosüsteemi sisenemiseks ja läbivaatuseks juhtudel, kui selle ülevõtmine pole vajalik ning nn virtuaalse viibimiskeelu rakendamiseks. Dokumentide nõudmisega seoses ilmnes, et problemaatiline on dokumendi mõiste sisustamine küberturvalisuse valdkonna eripära silmas pidades ja seetõttu vajaks täpsustamist, millist materjali on võimalik antud meetme rakendamisel välja nõuda. Samuti vajaks täpsustamist volitusnorm, millistel alustel on RIA õigustatud vallasasja hoiule võtma.

Lisaks püsitatud uurimisküsimustele vastamisele tehti käesolevas töös veel mõned täiendavad olulised järeldused. Esiteks pole küberturvalisuse seaduse eelnõuga lahendatud küsimust, milles seisneb RIA koordineeriv roll küberturvalisuse tagamisel. Eelnõus on sätestatud vaid üldine volitusnorm, kuid koordineerimise sisu ei muutu sellega selgemaks. Teiseks tuleks valdkonna reguleerimisega seotud osapooltel jõuda kokkuleppele kasutatavate mõistete sisus. Eelkõige oleks vaja defineerida küberturvalisuse mõiste sisu ja ulatus. Samuti tuleks küberturvalisuse seaduse eelnõus kasutatavad mõisted küberintsident, olulise mõjuga küberintsident ja oht selgelt siduda korrakaitseõiguse terminoloogiaga. Kuna Eesti õiguskorras on riiklik järelevalve korrakaitseõiguse keskne, siis tuleb ka küberturvalisuse tagamisel vastavast loogikast lähtuda. Mõistete sisu kokkuleppimise eesmärk on jõuda valdkonna olemuse ja piiride osas ühesuguse arusaama ja õigusliku käsitluseni.

Küberturvalisus on kiiresti arenev valdkond, mis esitab väljakutse ka selle õiguslikule reguleerimisele. Käesolevas magistritöös analüüsiti põhiõiguste ja -vabaduste kaitset Eestis esmakordselt küberturvalisuse tagamise seisukohast, seega töö väärtus seisneb temaatilise diskussiooni avamises. Kuna riigisisene valdkondlik regulatsioon on veel kujundamisel, siis on võimalik analüüsi kasutada õigusraamistiku väljatöötamisel ning vastavaid järeldusi arvesse võtta põhiõiguste ja -vabaduste kaitse paremaks tagamiseks. Magistritöö on kasutatav küberturvalisuse seaduse eelnõu seletuskirja täiendusena, samuti on võimalik selles esitatud ettepanekutest lähtuda eelnõu täiendamisel, näiteks defineerida küberturvalisuse mõiste. Küberturvalisuse valdkonna reguleerimine väärib rahvusvahelise õiguse keskse käsitluse kõrval enam uurimist riigisisese õiguse seisukohast. Edaspidi võiks osutuda asjakohaseks uurimisobjektiks teiste riikide küberturvalisuse alased regulatsioonid, kasutades võrdlevat analüüsimeetodit. Kuna analüüsiga ei antud küberturvalisuse tagamiseks rakendatavatele meetmetele hinnangut arvuti- või informatsiooni eetika seisukohast, siis oleks ka see üks võimalik edasine uurimisteema.

PROTECTION OF FUNDAMENTAL RIGHTS AND FREEDOMS IN EXTENDING STATE SUPERVISION MANDATE OF THE INFORMATION SYSTEM AUTHORITY IN ESTONIA

Summary

Rapid growth in the use of technology has provided us with a new kind of space – cyberspace. Cyberspace offers new opportunities while connecting devices and humans all over the world. Nevertheless, it also has brought up several kinds of new threats. Cyberspace could be defined as a technology-created reality. Further, the secure state of this technology-created reality – or cyber security – can be considered as a condition in which the risks affecting information processing tools are not realized. There are different kinds of malicious cyber activities. One of the most harmful ones would be a cyber-attack, which can cause death or injuries to many people. Nevertheless, not all malicious activities in cyberspace would pose a threat to one`s life or health. For example, ransomware can cause significant inconvenience, material or moral damage and other unwanted consequences to a victim. Undoubtedly, making cyberspace safe is in the interests of all states and societies. While it does not correspond to a common understanding of the public sphere, there is a need for debate on which measures are legitimate to take to ensure security in cyberspace.

Besides security issues, human rights are also considered as an essential part of modern democratic society. While information technology has provided us with new tools to practice democracy, there are also different ways to restrict one`s fundamental rights and freedoms while using it. In order to take measures for securing cyberspace, it shall be analysed thoroughly under what conditions and to what extent it is legitimate to restrict the fundamental rights and freedoms of an individual.

In current paper, the author analyses infringement of fundamental rights and freedoms in connection of ensuring cyber security. The focus of the Master's thesis is to determine if and to what extent the protection of fundamental rights and freedoms has been taken into account while preparing state supervision measures implemented by the Information System Authority in Estonia. The main goal is to find out which are the major threats in cyberspace and to assess the impact of the measures taken by the state according to the draft of the Cyber Security Act.

According to the hypothesis, there are extensive state supervision measures under preparation in Estonia, in order to ensure cyber security. However, not all of these measures are in balance with the state`s obligation to guard fundamental rights and freedoms. The analysis is based on the draft of the Cyber Security Act, which was in legal proceeding process while preparing the current thesis.

Three research questions are raised to check the hypothesis. First, the author examines what kind of threats affect cyber security and which law applies in these cases. Also, the issue of the limits of the Law Enforcement Act is one of the core elements of the analysis. Secondly, the author sets the question whether the state supervision measures are on the conformity with the Constitution. The last research question focuses on whether and which state supervision measures should be amended or supplemented in order to secure cyberspace as well as protect fundamental rights and freedoms. Qualitative analytical techniques are used in the paper.

The Master's thesis consists of three chapters. The first chapter gives an overview of the theoretical foundations of the Estonian Law Enforcement Act and protection of fundamental rights and freedoms based on the Constitution. Fundamental rights and freedoms are part of the national legal order as well as widely recognized principles at the international level. Protection of fundamental rights and freedoms in the Estonian legal system is guaranteed by the Constitution, which carries the fundamental idea of nature and functioning of the state. The Constitution has provided an obligation to protect fundamental rights and freedoms, but also a possibility of infringement of fundamental rights and freedoms, in order to ensure public order and national security. However, there must be a legal basis to justify any infringement. State supervision measures must be in each case justified by the law enforcement agency applying it and proportionate to the objective pursued.

The preamble to the Constitution emphasizes the task of protecting internal and external peace. While ensuring public order as one of the core legal interests, other fundamental rights of an individual can be legitimately restricted. In each case, this kind of intervention by the state authorities must be thoroughly assessed and legitimate. One of the most important and fundamental principles of the Constitution is the principle of proportionality, or the prohibition of using excessive power. It defines the conditions for limiting fundamental rights and freedoms. According to the Constitution, restrictions on fundamental rights and freedoms of an individual must be necessary in a democratic society. The Supreme Court has used a three-stage

proportionality test to assess the proportionality – the appropriateness, necessity and proportionality of the measure in the narrower sense.

In Estonia, state supervision is regulated by several acts, starting by the Constitution. The Law Enforcement Act is the core legal act of law enforcement and is supplemented by several field-specific legal acts. State supervision is based on the danger aversion law doctrine which includes prevention and aversion of threats. The aim is to guarantee internal security, as well as to protect the safety of people and inviolability of their legal interests as a constitutional value. When applying state supervision measures, it is important to distinguish between the measures aimed at prevention of threat (no specific threat or disruption) and the measures aimed at threat aversion (applied in case of a suspicion, threat or breach of public order). According to the Law Encorfement Act § 24 (1), a law enforcement agency is permitted to apply special state supervision measures for the prevention of a threat if a situation in the occurrence of which a threat will arise can be deemed possible based on a threat prognosis. The above is also applicable while ensuring security in cyberspace.

State supervision measures must be in accordance with the Constitution. It means that in case a state applies restrictive measures it must also consider the competing obligation to guarantee an individual`s fundamental rights and freedoms. The question arises whether fundamental rights and freedoms in cyberspace should be considered the same as in common public sphere. Application of the Law Enforcement Act is based on the premise that a cyber incident is considered as a breach of order. Therefore, ensuring fundamental rights and freedoms in cyberspace should be treated in the same way as in other areas of everyday life.

The second chapter focuses on threats in cyberspace and the corresponding law. The aim of the chapter is to identify the extent to which cyber security issues can be solved by state supervision. The United Nations Group of Governmental Experts has introduced three reports on the Developments in the Field of Information and Telecommunications in the Context of International Security (2010, 2013, and 2015). These reports highlight comprehensiveness of issues concerning information and communication technology. The risks associated with information and communication technologies have increased over time and have become global. Widespread usage of mobile devices, Web services, social networks and cloud computing makes cyber safety a growing challenge. Each technical tool connected to the internet is a hypothetical target for a misuse. Cyber-crime is therefore one of the fastest growing problems. The tools and methods created by criminals are a significant source of threat due to

increasing know-how, as society has become highly dependent on technology-driven infrastructures. Cyberspace is an attractive ground for conducting malicious activities due to global connectivity, as well as vulnerability and anonymity of technology. The Estonia's case is specific since the functioning of the state and society is strongly linked to the operation of e-services, which is why both random and targeted cyber-crime has become a growing source of threat. In addition, the geopolitical location and the activities of the neighbouring countries must be considered when assessing threats. The European Union Agency for Network and Information Security (ENISA) has identified several problems in cyberspace. In 2016, malware distribution, web-based attacks, web application attacks, denial of service attacks and botnets were reported as top five incident types. In the same period the Information System Authority registered malware (via e-mails and web pages) and botnet cases as the main types of cyber incidents in Estonia.

Malicious activities and offenses committed in cyberspace may constitute a problem both within and across the state`s borders. Every state is responsible for ensuring the legal order in its territory. For example, a person in the national territory suffers from an act of cyber-crime. This kind of an activity constitutes a threat and conflicts with the national legal order and the public interest in general, therefore the matter falls within the criterion of public order. According to the current thesis, law enforcement is particularly relevant for combating cyber-crime and securing vital services, and in a limited way fighting terrorism and cyber-espionage.

In this chapter, one part is also dedicated to explaining the legal terms of the Law Enforcement Act and its links to cyber security. Risk, public order, disorder, etc. defined in the Act are specific legal terms. Therefore, the terminology used in the field of cyber security should be in compliance with the Act.

The last chapter constitutes the most important part of the paper. Using the proportionality test, the author analysed state supervision measures in the field of cyber security in terms of protection of fundamental rights and freedoms. Each measure was assessed from the compatibility perspective with the Constitution. The author analysed eleven relevant norms in the Law Enforcement Act and the draft Cyber Security Act in detail. These norms contain general and special state supervision measures, which are applicable by the Information System Authority in order to ensure cyber security. The respective measures were: notification, precept and application of administrative coercive measure, countering of threat or elimination of disturbance by a law enforcement agency, questioning and requiring of documents, summons

and compelled attendance, confirmation of identity, processing of personal data by obtaining data from an electronic communication, prohibition on stay, entry into premises, examination of premises and taking a movable into storage. However, the final assessment of proportionality could be made when applying a measure in a specific situation, the Parliament should be convinced there are sufficient grounds for the protection of fundamental rights and freedoms when adopting the law. Therefore, the explanatory memorandum to the draft act should provide information which specific Estonian domestic measures are necessary to ensure cyber security and also contain sufficient analysis on the potential impact.

By conducting the proportionality test, the author evaluated each measure in the terms of appropriateness, necessity and proportionality in the narrower sense and, if necessary, suggested some supplementations. According to the analysis, none of the measures were directly in conflict with the Constitution. However, all the measures were in some respect problematic regarding infringement of fundamental rights and freedoms, including shortcomings in the justification of the measures. The explanatory memorandum to the draft Cyber Security Act indicated that the proportionality of the measures has been analysed in a very general way during the preparation process of the Act. The author recognized that fundamental freedoms of entrepreneurship, privacy, integrity of property, personal integrity and the general right to freedom were the most infringed ones.

Analyses of the United Nations and ENISA as well as analyses conducted by Estonian authorities` confirmed the diversity of threats in cyberspace from cyber-crime to the risk of military intervention. Depending on the nature of a problem, national or international law applies. As cyberspace is global, co-operation between states and a uniform interpretation of the international law is applicable to cyber security are vital to cope with threats. Nevertheless, regulation area of the Law Enforcement Act is limited to ensure cyber security and shall be supplemented by other regulations, e.g. data protection regulation, information systems` security measures.

The fundamental rights and freedoms guaranteed by the Constitution are in nature universal and therefore also apply in cyberspace. The same applies to infringement of fundamental rights and freedoms in cyberspace – when protecting other values of the constitutional order an infringement is allowed but must always be justified. However, the author found that the main problem is that there is still a lack of comprehensive view of the Estonian legal framework in the field of cyber security. In order to cope with threats, it is necessary to develop a clear and

common understanding on the methods how security in cyberspace can be ensured. It is also important to consider what kind of measures are legitimate and appropriate to apply in case of each type of threat.

Choice of restrictive measures, including state supervision measures, should be based on risk analysis and consequently, a comprehensive legal framework shall be developed to ensure security in cyberspace. However, under the European Union law, the Member States are responsible for ensuring cyber security and applying relevant measures. However, the choice of measures to achieve the goal should be based on analysis and be clearly justified, as the restrictive measures cause infringement of fundamental rights and freedoms. It is important to distinguish between threat prevention and threat aversion measures. In the first case, an infringement must be particularly justified. More precisely, it must be assessed to what extent it is possible to restrict one`s fundamental rights and freedoms so that the prevention of potential damage would not become a predicament of actions on behalf of state supervision. Therefore, certain measures may not be used for the risk prevention purposes.

The hypothesis of the Master`s thesis was confirmed. The draft Cyber Security Act enhances the Information System Authority`s mandate to implement specific state supervision measures. In the author's opinion, it will allow the Information System Authority to exercise sufficient state supervision to ensure cyber security. Although the analysis did not reveal a need for any new measures, some regulations of measures in the draft Cyber Security Act should be specified, e.g. the measure regulating entry and examination of the network and information system in cases it is unnecessary to take over the system by the Information System Authority.

In addition, there were some important findings more. First, the draft Cyber Security Act does not resolve the issue of the Information System Authority's coordinating role in ensuring cyber security in Estonia. Second, the parties involved should reach an agreement on the content of fundamental legal terms concerning cyber security. In particular, the content and scope of cyber security itself should be defined. Also, legal terms used in the draft Cyber Security Act (e.g. cyber incident, cyber incident with a significant impact, threat) shall be clearly linked to the terminology of the Law Enforcement Act, which is the main legal act regulating law enforcement in Estonia.

Fast developments in the field of information technology and cyber security challenge legal framework. The author conducted a scientific research on the protection of fundamental rights

and freedoms in connection with cyber security for the first time in Estonia. Thus, the value of the thesis is to open a thematic discussion. As Estonian domestic regulation concerning cyber security is still under development, it is possible to take the results of the analysis into account in further legislative process.

KASUTATUD KIRJANDUS

1. R. Alexy. Põhiõigused Eesti põhiseaduses. – Juridica 2001/eriväljaanne.
2. L. Floridi. The ethics of information. Oxford: Oxford University Press, 2013.
3. M. Ernits. Põhiõiguste mõiste ja tähtsus õigussüsteemis. – Juridica 1996/IX.
4. J. Ferejohn, P.Pasquino. The law of the exception: A typology of emergency powers. – Oxford University Press and New York University School of Law 2004, I.CON, Volume 2, Number 2, 2004.
5. E. Hirsnik. Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid. – Juridica 2014/VIII.
6. J. Jäätma. Ohutõrjeõigus politsei- ja korrakaitseõiguses: kooskõla põhiseadusega. Tartu: Tartu Ülikooli Kirjastus 2015.
7. J. Jäätma. The Constitutional Requirements for Averting of a Danger. – Juridica International 2012/XIX.
8. P.H. van Kempen. Four concepts of security. A human rights perspective. – Human Rights Law Review, March 2013, 13(1), lk 3, 7.
9. M. Laaring. Eesti korrakaitseõigus ohuennetusõigusena. Tartu: Tartu Ülikooli Kirjastus 2015.
10. M. Laaring, S. Pars, H. Kranich jt. Korrakaitseseadus: kommenteeritud väljaanne. Tallinn: Sisekaitseakadeemia, 2017.
11. Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 4. täiend. vlj. Tallinn: Juura, 2017.
12. W.B. Miller. Classifying and Cataloging Cyber-Security Indidents Within Cyber-Physical Systems. Brigham Young University, 2014. – https://scholarsarchive.byu.edu/etd/4345 (03.02.2018).
13. I. Pärnamägi. Avaliku korra mõiste Eesti ohutõrjeõiguses. – Juridica 2016/IV.
14. M. Roscini. Cyber operations and the use of force in international law. Oxford University Press, 2014.
15. P. Schasmin, C. Ginter. Lahendite Tele2 Sverige ja Digital Rights Ireland mõju sideandmete mugavkasutusele Eestis. – Juridica 2017/I.
16. M. N. Schmitt (gen.ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations : prepared by the International Groups of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press 2017.

17. F. Schoch, M. Ernits. Üldklausli vältimatus nüüdisaegses ohutõrjeõiguses. – Juridica 2010/VIII.
18. E. Tikk, A. Nõmper. Informatsioon ja õigus. Tallinn: Juura, 2007.

KASUTATUD ÕIGUSAKTID JA EELNÕUD

Eesti õigusaktid

1. Arhiiviseadus. – RT I, 06.01.2016, 6.
2. Asendustäitmise ja sunniraha seadus. – RT I, 12.07.2014, 29.
3. Asjaõigusseadus. – RT I, 25.01.2017, 4.
4. Avaliku teabe seadus. - RT I, 06.01.2016, 7.
5. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
6. Elektroonilise side seadus. - RT I, 23.03.2017, 6.
7. Haldusmenetluse seadus. - RT I, 25.10.2016, 5.
8. Hea õigusloome ja normitehnika eeskiri. VVm 22.12.2011 nr 180. – RT I, 29.12.2011, 228.
9. Hädaolukorra seadus. – RT I, 03.03.2017, 1.
10. Infosüsteemide turvameetmete süsteem. VVm 20.12.2007 nr 252. – RT I 2009, 6, 39.
11. Infoühiskonna teenuse seadus. – RT I, 12.07.2014, 48.
12. Isikuandmete kaitse seadus. – RT I, 06.01.2016, 10.
13. Julgeolekuasutuste seadus. – RT I, 05.05.2017, 2.
14. Kaitsepolitseiameti põhimäärus. SiMm 29.10.2014 nr 46. – RT I, 10.10.2017, 11.
15. Kaitseväe korralduse seadus. – RT I, 05.05.2017, 3.
16. Karistusseadustik. – RT I, 26.06.2017, 8
17. Korrakaitseseadus. – RT I, 02.12.2016, 6.
18. Kriminaalmenetluse seadustik. – RT I, 05.12.2017, 8.
19. „Küberjulgeoleku strateegia 2014–2017" ja selle rakendusplaani aastateks 2014–2017 heakskiitmine. VVk 17.09.2014 nr 390. – RT III, 19.09.2014, 3.
20. Lennundusseadus. – RT I, 03.03.2017, 16.
21. Rahvastikuregistri seadus. – RT I, 10.03.2017, 6.
22. Raudteeseadus. – RT I, 16.05.2017, 3.
23. Riigi Infosüsteemi Ameti põhimäärus. MKMm 25.04.2011 nr 28. – RT I, 29.12.2016, 14.
24. Sadamaseadus. – RT I, 03.03.2017, 24.
25. Tsiviilseadustiku üldosa seadus. – RT I, 12.03.2015, 106.
26. Tööstusomandi õiguskorralduse aluste seadus. – RT I, 28.12.2011, 46.

Rahvusvahelise õiguse allikad ja Euroopa Liidu aktid

27. Arvutikuritegevusvastane konventsioon. – RT II 2003, 9, 32.
28. Euroopa Liidu põhiõiguste harta. – ELT C 326, lk 391–407.
29. Euroopa Liidu Toimimise Leping. – ELT C 83.
30. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, lk 31–50; ELT eriväljaanne 13/15, lk 355–374.
31. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, lk 37–47 (ELT eriväljaanne 13/29, lk 514–524). Muudetud Euroopa Parlamendi ja nõukogu direktiiviga nr 2009/136/EÜ, 25. november 2009. – ELT L 337, lk 11–36.
32. Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. – ELT L 105, lk 54–63.
33. Nõukogu direktiiv 2008/114/EÜ, 8. detsember 2008, Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta. – ELT L 345, lk 75–82.
34. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. – ELT L 194, lk 1–30.
35. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57.
36. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. – RT II 1994, 10, 11.
37. The Universal Declaration of Human Rights. The UN General Assembly in Paris on 10th December 1948. – http://www.ohchr.org/EN/UDHR/Pages/UDHRIndex.aspx (22.12.2017).

Eelnõud

38. Küberturvalisuse seaduse eelnõu (kuupäevaga 03.10.2017 ametlikule kooskõlastamisele esitatud versioon). – https://eelnoud.valitsus.ee/main/mount/docList/e7ff643b-8b72-4a70-8f3e-dab03f9ca79f (21.04.2018).

KASUTATUD KOHTUPRAKTIKA

Riigikohtu praktika

1. RKKKo 3-1-1-95-06.
2. RKÜKo 3-1-1-116-09.
3. RKKKo 3-1-1-84-16.
4. RKTKo 3-2-1-152-09.
5. RKTKo 3-2-1-86-14.
6. RKÜKo 3-3-1-75-11.
7. RKHKo 3-3-1-80-11.
8. RKHKo 3-3-1-36-15.
9. RKHKo 3-3-1-75-15.
10. RKPJKo 3-4-1-6-00.
11. RKHKo 3-4-1-10-00.
12. RKPJKo 3-4-1-2-01.
13. RKPJKo 3-4-1-1-02.
14. RKPJKo 3-4-1-5-05.
15. RKÜKo 3-4-1-1-14.

Euroopa Kohtu praktika

16. EKo 12.06.2001, C-189/01, *H.Jippes*, p 81.
17. EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland*, p 42.
18. EKo 19.10.2016, C-582/14, Patrick Breyer versus Saksamaa Liitvabariik.
19. EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, Tele2 Sverige AB.

MUUD KASUTATUD ALLIKAD

1. Advokaadibüroo LEXTAL. Kübervaldkonna õigusanalüüs, 2016. – https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf (21.04.2018).
2. Advokaadibüroo SORAINEN. Riigi Infosüsteemi Ameti järelevalve meetmed haldusjärelevalvemenetluses ning häda- ja eriolukorras, 2017. – https://www.ria.ee/public/Kuberturvalisus/Oigusanalyys-2017-Sorainen.pdf (21.04.2018).
3. Cybernetica AS. Andmekaitse ja infoturbe leksikon. – http://akit.cyber.ee (21.04.2018).
4. Eesti Vabariigi Riigi Infosüsteemi Amet. Kriitilise informatsiooni infrastruktuuri kaitse. – https://www.ria.ee/ee/kiik.html (21.04.2018).
5. Eesti Vabariigi Riigi Infosüsteemi Amet. Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2015. aasta kokkuvõte. – https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html (21.04.2018).
6. Eesti Vabariigi Riigi Infosüsteemi Amet. Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte. – https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html (21.04.2018).
7. Eesti Vabariigi Kaitseministeerium. „Riigikaitse arengukava 2013 – 2022 mittesõjalised osad“ avalik kokkuvõte. – http://www.kaitseministeerium.ee/riigikaitse2022/laiapohjaline-riigikaitse/index.html (21.04.2018).
8. Eesti Vabariigi Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2015. – https://kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html (21.04.2018).
9. Eesti Vabariigi Kaitsepolitseiamet. Kaitsepolitseiameti aastaraamat 2016. – https://kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html (21.04.2018).
10. Eesti Vabariigi Majandus- ja Kommunikatsiooniministeerium. Küberjulgeoleku strateegia 2014–2017. – https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (21.04.2018). Küberjulgeoleku strateegia lisa 2. – https://www.mkm.ee/sites/default/files/lisa_2_valdkondlik_metoodika.doc (21.04.2018).

11. Eesti Vabariigi Riigikohus. Arvamus korrakaitseseaduse muutmise ja rakendamise seaduse eelnõu (424 SE) kohta. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/arvamused/2445bcfe-b04d-40c8-932e-db51253abea3/Korrakaitseseaduse%20muutmise%20ja%20rakendamise%20seadus (21.04.2018).
12. Eesti Vabariigi Siseministeerium. Siseministeeriumi eesmärk ja tegevused. Sisejulgeoleku tagamine. – https://www.siseministeerium.ee/et/siseturvalisuse-valdkond/sisejulgeoleku-tagamine (21.04.2018).
13. Eesti Vabariigi Siseministeerium. Elutähtsad teenused. – https://www.siseministeerium.ee/et/eesmark-tegevused/kriisireguleerimine/elutahtsad-teenused (21.04.2018).
14. Eesti Vabariigi Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2017. - https://www.valisluureamet.ee/hinnang.html (21.04.2018).
15. Eesti õigekeelsussõnaraamat: ÕS 2013. – Tallinn: Eesti Keele Sihtasutus 2013.
16. European Union Agency for Network and Information Security. ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends. – https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (21.04.2018).
17. H. Lõugas. Üle maailma levis reedel suur krüptolunavara laine. – https://geenius.ee/uudis/ule-maailma-levib-suur-kruptolunavara-laine/ (21.04.2018).
18. Korrakaitseseaduse eelnõu seletuskiri. 49 SE I. – https://www.riigikogu.ee/tegevus/eelnoud/eelnou/8a9c2286-06fc-65d2-957b-bd9e11a940c4/Korrakaitseseadus (21.04.2018).
19. Küberturvalisuse seaduse eelnõu seletuskiri (kuupäevaga 03.10.2017 ametlikule kooskõlastamisele esitatud versioon). – https://eelnoud.valitsus.ee/main/mount/docList/e7ff643b-8b72-4a70-8f3e-dab03f9ca79f (21.04.2018).
20. United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201). United Nations General Assembly, 2010. – https://undocs.org/A/65/201 (21.04.2018).
21. United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

(A/68/98*). United Nations General Assembly, 2013. – https://undocs.org/A/68/98 (21.04.2018).

22. United Nations. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). United Nations General Assembly, 2015. – https://undocs.org/A/70/174 (21.04.2018).
23. Wikipedia. WannaCry ransomware attack. – https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (21.04.2018).

LISA. Kokkuvõte küberturvalisust ohustavatest suundumustest ja olulisemad õigusallikad

Ohustav tegevus/suundumus	Eesmärk	Allikas*	Sihtmärk*	Olulisemad õigusallikad
Küberkuritegevus	Materiaalne kasu	G, I	I	RÕ: KarS, KorS RVÕ: arvutikuritegevusvastane konventsioon
Terrorism	Poliitiline, materiaalne kasu	G, I	R	RÕ: KarS, seadused konventsioonide ratifitseerimiseks, KorS RVÕ: valdkondlikud konventsioonid
Kriitilise infrastruktuuri ja elutähtsate teenuste osutamise kahjustamine	Kahju põhjustamine, ühiskonna destabiliseerimine	R, G	R	RÕ: HOS, ESS, KorS RVÕ: riigivastutuse õigus, EL direktiivid 2008/114/EÜ, 2016/1148
Küberrünne, kübersõda	Kahju põhjustamine, ühiskonna destabiliseerimine	R (G)	R	RÕ: ErSS, RiKS RVÕ: eelkõige ÜRO harta, Põhja-Atlandi leping
Küberspionaaž	(Salajase) info hankimine ja sellest kasu saamine	R	R, G	RÕ: JAS, KKS, AvTS, ISKE määrus, intellektuaalomandi kaitse õigus, KorS
Poliitiline mõjutustegevus, sabotaaž	Ühiskonna destabiliseerimine	R (G)	R (G, I)	-
IKT nn tagaustega programmeerimine	Manipuleerimine	G, I	R, G, I	-
Kõrgetasemeliste tööriistade ja tehnikate arendamine ja levitamine	Materiaalne kasu, kahju põhjustamine	G, I	R, G, I	-
Puhverserverite kasutamine	Tegevuse jälgede peitmine	G, I	R, G, I	-
Väär ründetegevuse omistamine (omistamisprobleem)	-	R	R	RVÕ: riigivastutuse õigus
IKT võimekuse erinemine riigiti	-	R	R	-
IKT arendamine sõjalisel otstarbel	Ründevõime arendamine	R	R	-
Mõjude ilmnemise kiirus ja ootamatus	-	R, G, I	R, G, I	-
IKT kasutusala laienemine, esemevõrk	-	I (R, G)	I	-

Tabel. Küberturvalisust ohustavad suundumused ja kohalduv õigus

* R-riik, G-isikute grupp/riigiväline osapool, I-indiviid;
**RÕ-riigisisene õigus, RVÕ – rahvusvaheline õigus

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Helen Ojamaa-Muru,

(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
„Põhiõiguste ja -vabaduste kaitse Riigi Infosüsteemi Ameti järelevalve volituste laiendamisel“,
(*lõputöö pealkiri*)

mille juhendaja on Eneken Tikk,
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, 23.04.2018